网络运维纪实文学

36个实例——源自真实
一线运维师的血泪情仇

网络运维

亲历记

王刚耀 著

清华大学出版社

网络运维亲历记

王刚耀　著

清华大学出版社

北　京

内 容 简 介

本书共包括 8 章，36 个网络运维实例。首先介绍常用的网络二、三层协议，包括 IP、HSRP、GVRP、VTP 协议和 Trunk 技术及网络运维中的一些技巧，如最简单的 Ping 和 Telnet 工具等。其次介绍当前用户比较关注的网络问题和热门的网络技术，如网络安全、虚拟化、IPv6 和无线网络等。最后介绍与网络运维相关的其他计算机应用技术，如应用系统和网络排查工具等。

本书深入浅出地介绍了计算机网络的多方面知识，注重应用实践，可作为网络从业人员的专业学习和参考用书，也可供高校计算机、通信、网络等专业的师生阅读参考。

图书在版编目(CIP)数据

网络运维亲历记 / 王刚耀著. — 北京：清华大学出版社，2016
ISBN 978-7-302-42984-5

Ⅰ. ①网… Ⅱ. ①王… Ⅲ. ①计算机网络—安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2016)第 030499 号

责任编辑：栾大成
装帧设计：
责任校对：徐俊伟
责任印制：

出版发行：清华大学出版社

网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn

印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：188mm×260mm　　**印　　张：**20.75　　**字　　数：**340 千字
版　　次：2016 年 7 月第 1 版　　**印　　次：**2016 年 7 月第 1 次印刷
印　　数：1～3500
定　　价：59.00 元

产品编号：066329-01

前 言

计算机技术和网络技术的高速发展，对人类社会各个方面的影响还在不断加深和发酵：从博客、BBS、微博到时下流行的微信；从电脑台式机、一体机、笔记本电脑到现在的平板电脑和移动终端；从现金支付、刷卡支付到网上支付和现在的扫码支付；从商场购物到网上购物等，都能看到计算机技术和网络技术的发展对人们生活的影响无处不在。

笔者从20世纪90年代上大学，及后来攻读硕士学位时，学习的都是计算机专业。毕业后工作直到现在，一直从事计算机和网络相关的工作，接触到了局域网、园区网、城域网和跨区域网的设计、实现和管理的全过程，经历了从局域网到互联网那激动人心的变化。

目前，计算机网络技术方面的书籍往往只介绍某一方面的技术，而且大多数书籍偏重于原理、理论方面知识，这对操作和实践性非常强的网络运维来说，是一个很大的缺憾。尤其对于在校的大学生，因为学校客观环境的限制，不可能拥有像在公司和企业中的实际网络环境，学习的参考书也是包含过多的理论知识，学习起来常常是一头雾水，摸不着头脑。而计算机网络知识的学习，必须通过真实项目的全过程实践，才能真正地掌握网络理论知识。

本书是笔者在多年的网络运维实践中逐渐总结积累下来的经验所得，读者只需对照书中的每一个运维实例的操作步骤，一步步操作，就可以解决相同或类似的网络故障。同时，在操作完成后，包含于其中的计算机网络知识也会了然于胸。

本书共包括8章内容，第1～3章介绍了常用的网络二、三层协议，包括IP、HSRP、GVRP、VTP协议和Trunk技术，以及网络运维中的一些技巧，如最简单的Ping和Telnet工具等。第4～6章介绍了当前用户比较关注的网络问题和热门的网络技术，如网络安全、虚拟化、IPv6和无线网络等。第7～8章介绍了和网络运维相关的其他计算机应用技术，如应用系统和网络排查工具等。

一个人的进步离不开周围人的关心和帮助，在此感谢我的家人，一直以来对我工作的支持；感谢我的同事们，在我工作遇到困难时，总是替我排忧解难；也感谢本书的编辑栾大成，要是没有他的“金点子”及合理的建议，本书也不会这么快和大家见面的。

由于笔者水平和经验有限，书中还存在不少缺点和不足，敬请广大读者批评指正，万分感谢！

网络运维这点事

目前，绝大多数单位运行的计算机网络都是基于TCP/IP协议的，若网络是无线网络，则在二层是基于802.11协议的，例如，使用最普遍的移动终端手机、平板电脑、笔记本电脑等接入到无线局域网WLAN，也就是接入到WIFI，这些终端上肯定会拥有一个IP地址，移动终端和无线路由器或者无线AP的连接通信方式就是使用802.11方式的。

若用户是使用台式机通过网线或光纤连接到网络上网时，台式机上也肯定会有一个IP地址，台式机通过办公室中的信息点再连接到交换机上，台式机和交换机之间的数据通信在二层上就是使用802.3协议的。

上面列举的用户终端通过两种不同的连接方式访问网络时，虽然它们在二层上使用的协议和技术是不一样的，但它们在三层、四层上运行的方式，或使用的协议是完全一致的，三层上主要就是IP协议，它最主要的特征就是每台终端上的IP地址。四层上主要就是TCP和UDP协议，最主要的特征就是端口号，TCP和UDP的端口号范围都是1～65535。

上面说了很多“二、三层”的事，那一层是干什么的？一层就是物理层，像上面说的台式机通过网线或光纤连接到交换机，网线、光纤和交换机上的电口、光口等，这些都是一层即物理层上的。

那网络运维师的日常工作范围，基本上就在这一～四层，如图0-1所示。若是连接到电脑上的网线接触不好导致用户不能访问网络，那就是一层和二层出问题了；若是用户终

端的IP地址有错误，那是三层有问题了；若是有用户反映他访问办公应用系统正常，但是访问不了财务应用系统，那有可能就是四层出问题了，因为应用系统都是和端口进行关联的。有的应用系统能够正常使用，有的不正常，那说明网络没有问题，网络是通的，有一种可能就是网络中的防火墙把财务应用系统的端口进行了限制和阻止，而没有限制和阻止办公应用系统的，所以就有了上面的故障现象。

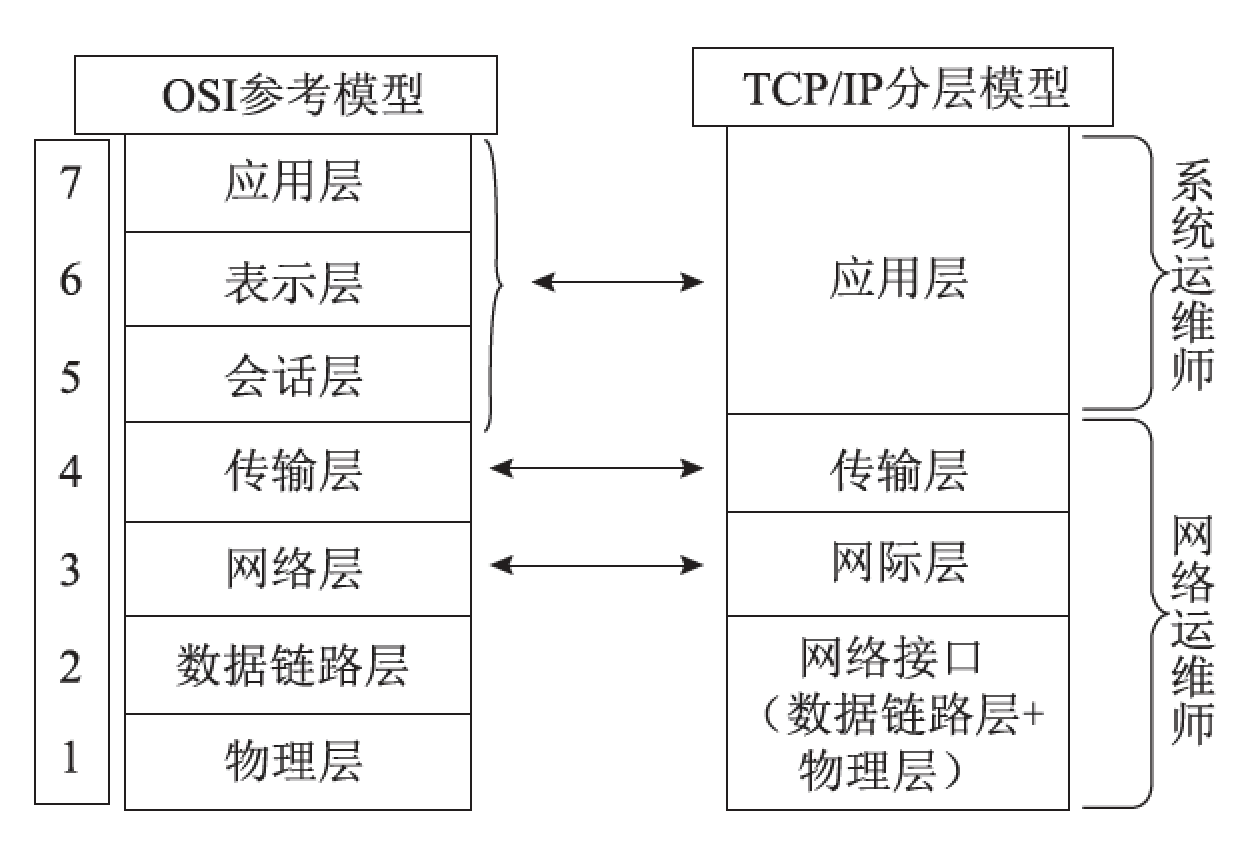
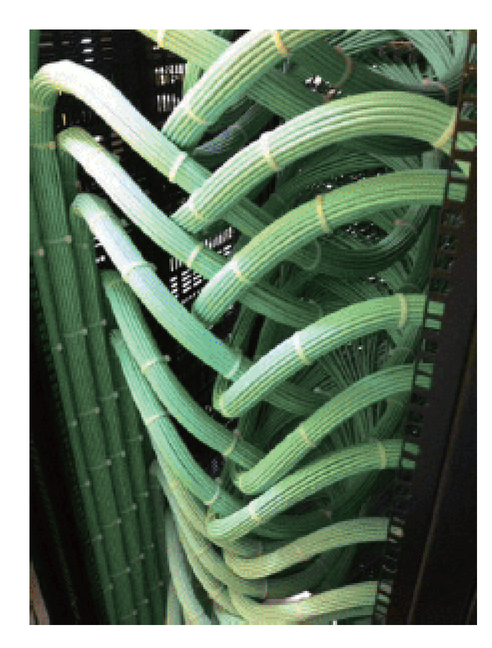


图0-1 运维工程师工作范围

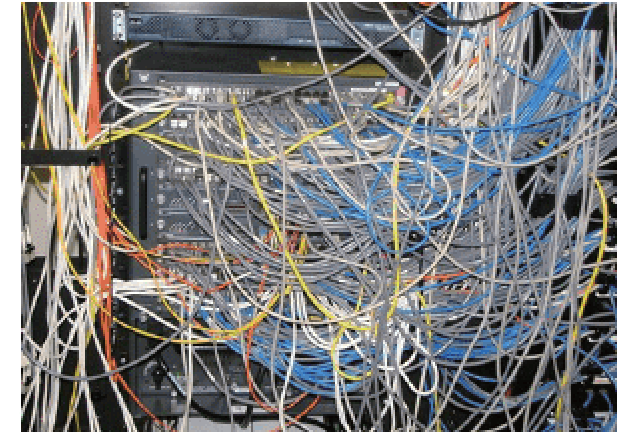
曾经微信上有一篇很火的文章，标题是《有一种机房叫别人家的机房》，文章主要是用图片的形式进行讲述的，我这里拣其中对比明显的几张贴上来：

人家家的





咱家的


对比是很明显的，这也从一个侧面说明，国内一些网络机房确实是存在管理疏松，在布线、接线上不严谨，不按要求和标准来，私拉乱扯。不过这几张图的对比也有些太夸张了，我们大部分的机房布线还是很整齐、很漂亮的，不比国外“人家家的”差，有些甚至还要比他们的好。

另外，我想说的是，就是通过这几张图，能够很直观地呈现出网络运维师的工作环境。这几张图显示的一般都是单位的中心机房，也是网络运维师的主要工作场所。其他的还有各个楼的分中心机房及每栋楼每层的网络设备间。另外，和网络终端用户及网络安全设备供应商的工程师进行交流、沟通和学习，也是网络运维师日常工作的一部分。

好了，说了这么多云里雾里的东西，也不知大家能看明白吗？下面就分8章36个实例具体说说网络运维师都干些什么事。

目　录

第1章 网络三层协议

其实，在互联网中用到的网络协议最多的就是TCP/IP协议，TCP/IP是Transmission Control Protocol/Internet Protocol的简写，中译名为传输控制协议/因特网互联协议。现在我们上班所在的公司和办公室，包括常常拿在手上的手机都连入了互联网。若是还没有联网，那就实在太落伍了。每天一上班，坐在办公桌前，打开电脑浏览器开始看邮箱和今天的新闻时，TCP/IP协议在你的电脑中就开始起作用了。

现在，英语是世界上最通用的语言，无论你到哪一个国家，只要你和对方都会说英语，那你们之间就可以进行对话交流了。同样，在Internet中，只要连入其中的终端遵守TCP/IP协议，它就可以和连入Internet中的其他终端进行通信了。也就是说TCP/IP协议组就类似一门语言。

TCP/IP协议又名网络通信协议，是Internet最基本的协议，也是Internet国际互联网络的基础。TCP/IP 定义了电子设备如何连入因特网及数据如何在它们之间传输的标准。协议采用了4层的层级结构，每一层都呼叫它的下一层所提供的协议来完成自己的需求。通俗而言：TCP负责发现传输的问题，一有问题就发出信号，要求重新传输，直到所有数据安全正确地传输到目的地。而IP是给因特网的每一台联网设备规定一个地址。

TCP/IP协议不是TCP和IP这两个协议的合称，而是指因特网整个TCP/IP协议族。从协议分层模型方面来讲，TCP/IP由4个层次组成：网络接口层、网络层、传输层、应用层。

TCP/IP协议并不完全符合OSI(Open System Interconnect)的7层参考模型，OSI是传统的开放式系统互连参考模型，是一种通信协议的7层抽象的参考模型，其中每一层执行某一特定任务。该模型的目的是使各种硬件在相同的层次上相互通信。这7层是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。而TCP/IP通信协议采用了四层的层级结构，每一层都呼叫它的下一层所提供的网络来完成自己的需求。

1.1 网络三层协议概述

1.1.1 IP协议

IP(Internet Protocol)，网络之间互连的协议，是为计算机网络相互连接进行通信而设计的协议。在因特网中，它是能使连接到网上的所有计算机网络实现相互通信的一套规则，规定了计算机在因特网上进行通信时应当遵守的规则。任何厂家生产的计算机系统，只要遵守IP协议就可以与因特网互连互通。

IPv6是Internet Protocol Version 6的缩写，它是IETF(Internet Engineering Task Force，互联网工程任务组)设计的用于替代现行版本IPv4的下一代IP协议。

IPv4地址分为5类：A类保留给政府机构，B类分配给中等规模的公司，C类分配给任何需要的人，D类用于组播，E类用于实验。各类可容纳的地址数目不同。当将IP地址写成二进制形式时，A类地址的第1位总是0，B类地址的前2位总是10，C类地址的前3位总是110。

1. A类地址

(1)A类地址第1字节为网络地址，其他3个字节为主机地址。它的第1个字节的第1位固定为0。

(2)A类地址网络号范围：1.0.0.0～126.0.0.0。

(3)A类地址中的私有地址和保留地址如下：

①10.X.X.X是私有地址(在互联网上不使用，而被用在局域网络中的地址)。范围为10.0.0.0～10.255.255.255。

②127.X.X.X是保留地址，用作循环测试。

2. B类地址

(1)B类地址第1字节和第2字节为网络地址，其他2个字节为主机地址。它的第1个字节的前2位固定为10。

(2)B类地址网络号范围：128.0.0.0～191.255.0.0。

(3)B类地址的私有地址和保留地址如下：

①172.16.0.0～172.31.255.255是私有地址。

②169.254.X.X是保留地址。如果你的IP地址是自动获取IP地址，而在网络上又没有找到可用的DHCP服务器，就会获取其中一个IP地址。

3. C类地址

(1)C类地址第1字节、第2字节和第3个字节为网络地址，第4个字节为主机地址。另外第1个字节的前3位固定为110。

(2)C类地址网络号范围：192.0.0.0～223.255.255.0。

(3)C类地址中的私有地址如下：

192.168.X.X(192.168.0.0～192.168.255.255)是私有地址。

4. D类地址

(1)D类地址不分网络地址和主机地址，它的第1个字节的前4位固定为1110。

(2)D类地址范围：224.0.0.0～239.255.255.255。

5. E类地址

(1)E类地址不分网络地址和主机地址，它的第1个字节的前5位固定为11110。

(2)E类地址范围：240.0.0.0～255.255.255.254。

IP地址如果只使用ABCDE类来划分，会造成大量的浪费。比如一个有500台主机的网络，无法使用C类地址。但如果使用一个B类地址，6万多个主机地址只有500个被使用，造成IP地址的大量浪费。因此，IP地址还支持VLSM(Variable Length Subnet Mask，可变长子网掩码)技术，可以在ABC类网络的基础上，进一步划分子网。

1.1.2 热备份协议

1. HSRP

HSRP(Hot Standby Router Protocol)热备份路由器协议，是思科的私有协议。

该协议中含有多台路由器，对应一个HSRP组。该组中只有一个路由器承担转发用户流量的职责，这就是活动路由器。当活动路由器失效后，备份路由器将承担该职责，成为新的活动路由器。

但是在本网络内的主机看来，虚拟路由器没有改变。所以主机仍然保持连接，没有受到故障的影响，这样就较好地解决了路由器切换的问题，这就是热备份的原理。

为了减少网络的数据流量，在设置完活动路由器和备份路由器之后，只有活动路由器和备份路由器定时发送HSRP报文。如果活动路由器失效，备份路由器将接管成为活动路由器。如果备份路由器失效或者变成了活动路由器，将由另外的路由器接管成为备份路由器。

负责转发数据包的路由器称之为活动路由器(Active Router)，一旦主动路由器出现故障，HSRP将激活备份路由器(Standby Routers)取代主动路由器。HSRP协议提供了一种决定使用主动路由器还是备份路由器的机制，并指定一个虚拟的 IP 地址作为网络系统的缺省网关地址。如果主动路由器出现故障，备份路由器(Standby Routers)承接主动路由器的所有任务，并且不会导致主机连通中断现象。

HSRP 运行在UDP上，采用端口号1985。路由器转发协议数据包的源地址使用的是实际IP地址，而并非虚拟地址，正是基于这一点，HSRP 路由器间能相互识别。

HSRP协议利用一个优先级方案来决定哪个配置了HSRP协议的路由器成为默认的主动路由器。如果一个路由器的优先级设置的比所有其他路由器的优先级高，则该路由器成为主动路由器。路由器的缺省优先级是100，所以如果只设置一个路由器的优先级高于100，则该路由器将成为主动路由器。

通过在设置了HSRP协议的路由器之间发组播(地址为224.0.0.2)来得知各自的HSRP优先级，HSRP协议选出当前的主动路由器。当在预先设定的一段时间内主动路由器不能发送Hello消息时，优先级最高的备用路由器变为主动路由器。路由器之间的包传输对网络上的所有主机来说都是透明的。

配置了HSRP协议的路由器交换以下3种组播消息：

Hello消息：Hello消息通知其他路由器发送路由器的HSRP优先级和状态信息，HSRP路由器默认为每3秒钟发送一个Hello消息。

Coup消息：当一个备用路由器变为一个主动路由器时发送一个coup消息。

Resign消息：当主动路由器要宕机或者当有优先级更高的路由器发送Hello消息时，主动路由器发送一个Resign消息。

HSRP的两个定时器：

HSRP使用两个定时器，Hello间隔和Hold间隔。默认的Hello间隔是3秒，默认的Hold间隔是10秒。Hello间隔定义了两组路由器之间交换信息的频率。Hold间隔定义了经过多长时间后，没有收到其他路由器的信息，则活动路由器或者备用路由器就会被宣告为失败。配置计时器并不是越小越好，虽然计时器越小则切换时间越短。计时器的配置需要和STP等的切换时间相一致。另外，Hold间隔最少应该是Hello间隔的3倍。

在任一时刻，配置了HSRP协议的路由器都将处于以下6种状态之一：

Initial状态：HSRP启动时的状态，HSRP还没有运行，一般是在改变配置或端口刚刚启动时进入该状态。

Learn状态：学习状态，不知道虚拟IP，未看到活跃路由器发Hello，等待活动路由器发hello。

Listen状态：路由器已经得到了虚拟IP地址，但是它既不是活动路由器也不是等待路由器。它一直监听从活动路由器和等待路由器发来的Hello报文。

Speak状态：在该状态下，路由器定期发送Hello报文，并且积极参加活动路由器或等待路由器的竞选。

Standby状态：当主动路由器失效时路由器准备接管包传输功能。

Active状态：路由器执行包传输功能。

2. VRRP

VRRP(Virtual Router Redundancy Protocol)虚拟路由冗余协议，是由IETF(国际互联网工程任务组)提出的解决局域网中配置静态网关出现单点失效现象的路由协议。

VRRP是一种选择协议，它可以把一个虚拟路由器的责任动态分配到局域网上的 VRRP 路由器中的一台。控制虚拟路由器IP地址的 VRRP 路由器称为主路由

器，它负责转发数据包到这些虚拟IP地址。一旦主路由器不可用，这种选择过程就提供了动态的故障转移机制，这就允许虚拟路由器的IP地址可以作为终端主机的默认第一跳路由器。一个局域网络内的所有主机都设置缺省网关，这样主机发出的目的地址不在本网段的报文将被通过缺省网关发往三层交换机，当缺省路由器Down掉(端口关闭)之后，如果路由器设置了VRRP时，那么这时，虚拟路由将启用备份路由器，从而实现了主机和外部网络的通信。

VRRP 将局域网的一组路由器，包括一个Master(活动路由器)和若干个Backup(备份路由器)，组织成一个虚拟路由器，称之为一个备份组。这个虚拟的路由器拥有自己的IP 地址，例如10.100.10.1，这个IP 地址可以和备份组内的某个路由器的接口地址相同，相同的则称为IP拥有者，备份组内的路由器也有自己的IP 地址，例如Master的IP 地址为10.100.10.2，Backup 的IP 地址为10.100.10.3。局域网内的主机仅仅知道这个虚拟路由器的IP 地址10.100.10.1，而并不知道具体的Master 路由器的IP 地址10.100.10.2 以及Backup 路由器的IP 地址10.100.10.3。它们将自己的缺省路由下一跳地址设置为该虚拟路由器的IP 地址10.100.10.1。于是，网络内的主机就通过这个虚拟的路由器来与其他网络进行通信。如果备份组内的Master 路由器坏掉，Backup 路由器将会通过选举策略选出一个新的Master 路由器，继续向网络内的主机提供路由服务。从而实现网络内的主机不间断地与外部网络进行通信。

3. GLBP

GLBP(Gateway Load Balancing Protocol)网关负载均衡协议，是思科的专有协议。和HSRP、VRRP不同的是，GLBP不仅提供冗余网关，还在各网关之间提供负载均衡，而HSRP、VRRP都必须选定一个活动路由器，而备用路由器则处于闲置状态。GLBP可以绑定多个MAC地址到虚拟IP，从而允许客户端通过获得不同的虚拟MAC地址，通过不同的路由器转发数据，因为客户端利用的地址是解析到的虚拟的MAC地址，而网关地址仍使用相同的虚拟IP，从而不但实现了冗余还能够负载均衡。

1)活动网关选举

使用类似于HSRP的机制选举活动网关，优先级最高的路由器成为活动路由器，若优先级相同则IP地址最高的路由器成为活动路由器。称作Active Virtual Gateway，其他非AVG提供冗余。某路由器被推举为AVG后，和HSRP不同的工

作开始了，AVG分配虚拟的MAC地址给其他GLBP组成员。所有的GLBP组中的路由器都转发包，但是各路由器只负责转发与自己的虚拟MAC地址的相关的数据包。GLBP成员之间通过每3秒钟向组播地址为224.0.0.102的UDP端口3222发送Hello数据包，来进行通信。

2)地址分配

每个GLBP组中最多有4个虚拟MAC地址，非AVG也被称作Active Virtual Forwarde(AVF)，非AVG路由器由AVG按序分配虚拟MAC地址。AVF分为两类：Primary Virtual Forwarder和Secondary Virtual Forwarder。直接由AVG分配虚拟MAC地址的路由器被称作Primary Virtual Forwarder，后续不知道AVG真实IP地址的组成员，只能使用Hello包来识别其身份，然后被分配虚拟MAC地址，此类被称作Secondary Virtual Forwarder。

3)GLBP配置

如果AVG失效，则推举就会发生，决定哪个AVF替代AVG来分配MAC地址，推举机制依赖于优先级。最多可以配置1个GLBP组，不同的用户组可以配置成使用不同的组AVG来作为其网关。

```
Cisco#configure terminal
Cisco(config)#track 100 int f0/0 line-protocol
//定义跟踪目标100为f0/0接口的二层故障
Cisco(config-if)#exit
Cisco(config)#int fastethernet 0/0
Cisco(config-if)#ip address 10.1.1.1
Cisco(config-if)#glbp 99 ip 10.1.1.254
Cisco(config-if)#glbp 99 name TEST
//配置GLBP名字，可选
Cisco(config-if)#glbp 99 timers 3 10
```

```
  //配置GLBP的Hello时间3秒和Hold时间10秒
Cisco(config-if)#glbp 99 priority 105
//配置优先级，默认是100，这里为105
Cisco(config-if)#glbp 99 preempt
//配置GLBP的路由器会进行AVG抢占，否则priority再高也不抢占
Cisco(config-if)#glbp 99 preempt delay minimum 10
  //配置AVG的抢占延时10秒
Cisco(config-if)#glbp 99 weighting track100 decrement 50
//当跟踪目标100出现故障的时候权重减50
Cisco(config-if)#exit
```

4)GLBP的特性

负载分担：管理员可以通过配置GLBP，使多台路由器共同承载局域网客户端的流量，从而在多台可用路由器之间实现更为公平的负载均衡。

多虚拟路由器：GLBP在一台路由器的每个物理接口上，支持多达1024个虚拟路由器，即GLBP组，每个组最多支持4个虚拟转发者。

抢占：GLBP的冗余性机制允许当具有更高优先级的备用虚拟网关变得可用后，通过抢占机制成为AVG。转发者的抢占行为与此相似，只是转发者抢占使用的是加权而不是优先级，且默认启用。

有效的资源利用：GLBP使组中的每台路由器都可以充当备用角色，而不需要部署一台专用的备用路由器，因为所有可用的路由器都可以承载网络流量。

5)GLBP的运作

GLBP协议支持3种负载均衡方式，下面是配置GLBP负载均衡时，对3个参数的解释。

Cisco(config-if)#glbp group load-balancing [round-robin | weighted | host-

dependent]

round-robin：Load balance equally using each forwarder in turn。

weighted： Load balance in proportion to forwarder weighting。

host-dependent： Load balance equally, source MAC determines forwarder choice。

第一：根据ARP请求轮询。循环负载分担算法：当客户端发送ARP请求来解析默认网关的MAC地址时，每个客户端接收到的ARP响应中包含的MAC地址，是循环算法中下一个可用路由器的MAC地址。所有路由器的MAC地址会被按顺序放入地址解析响应中，作为默认网关IP地址对应的MAC地址返回给客户端。

第二：根据路由器的权重分配，权重越高被分配的可能性越大。加权负载分担算法：被定向到一台路由器的负载量取决于该路由器所通告的加权值。

第三：根据不同主机的源MAC地址。主机相关负载分担算法：只要某个虚拟MAC地址还在GLBP组中参与流量转发，就确保某主机总是使用这个虚拟MAC地址进行通信。

1.1.3 DHCP协议

DHCP(Dynamic Host Configure Protocol，动态主机配置协议)，是一个局域网的网络协议，使用UDP协议工作，主要有两个用途：一是给内部网络或网络服务供应商自动分配IP地址，二是给用户或者内部网络管理员作为对所有计算机作中央管理的手段。DHCP有3个端口，其中UDP 67和UDP 68为正常的DHCP服务端口，分别作为DHCP Server和DHCP Client的服务端口。

在一个使用TCP/IP协议的网络中，每一台计算机都必须至少有一个IP地址，才能与其他计算机连接通信。为了便于统一规划和管理网络中的IP地址，DHCP应运而生了。这种网络服务有利于对校园网络中的客户机IP地址进行有效管理，而不需要一个一个手动指定IP地址。

DHCP用一台或一组DHCP服务器来管理网络参数的分配，这种方案具有容错性。即使在一个仅拥有少量机器的网络中，DHCP仍然是有用的，因为一台机

器可以几乎不造成任何影响地被增加到本地网络中。

甚至对于那些很少改变地址的服务器来说，DHCP仍然被建议用来设置它们的地址。如果服务器需要被重新分配地址的时候，就可以在尽可能少的地方去做这些改动。对于一些设备，如路由器和防火墙，则不应使用DHCP。把TFTP或SSH服务器放在同一台运行DHCP的机器上也是有用的，目的是为了集中管理。

DHCP也可用于直接为服务器和桌面计算机分配地址，并且通过一个PPP代理，也可为拨号及宽带主机及住宅NAT网关和路由器分配地址。DHCP一般不适用于使用在无边际路由器和DNS服务器上。

1.1.4　NAT技术

NAT(Network Address Translation)网络地址转换，当在专用网内部的一些主机本来已经分配到了本地IP地址，但现在又想和因特网上的主机通信时，可使用NAT方法。NAT的实现方式有3种：静态转换(Static NAT)、动态转换(Dynamic NAT)和端口多路复用(Port Address Translation)。

静态NAT设置起来最为简单，内部网络中的每个主机都被永久映射成外部网络中的某个合法的地址。静态转换是指将内部网络的私有IP地址转换为公有IP地址，IP地址对是一对一的，是一成不变的，某个私有IP地址只转换为某个公有IP地址。借助于静态转换，可以实现外部网络对内部网络中某些特定设备如服务器的访问。

动态NAT是指将内部网络的私有IP地址转换为公用IP地址时，IP地址是不确定的，是随机的，所有被授权访问上Internet的私有IP地址可随机转换为任何指定的合法IP地址。也就是说，只要指定哪些内部地址可以进行转换以及用哪些合法地址作为外部地址时，就可以进行动态转换。动态转换可以使用多个合法外部地址集。当ISP提供的合法IP地址略少于网络内部的计算机数量时，就可以采用动态转换的方式。

端口多路复用是指改变外出数据包的源端口并进行端口转换，即端口地址转换。内部网络的所有主机均可共享一个合法外部IP地址实现对Internet的访问，从而可以最大限度地节约IP地址资源。同时，又可隐藏网络内部的所有主机，有效避免来自Internet的攻击。因此，目前网络中应用最多的就是端口多路复用方式。

在配置网络地址转换的过程之前，首先必须搞清楚内部接口和外部接口，以及在哪个外部接口上启用NAT。通常情况下，连接到用户内部网络的接口是NAT内部接口，而连接到外部网络的接口是NAT外部接口。

假设内部局域网使用的IP地址段为192.168.0.1～192.168.0.254，路由器局域网端(默认网关)的IP地址为192.168.0.1，子网掩码为255.255.255.0。网络分配的合法IP地址范围为61.159.62.128～61.159.62.135，路由器在广域网中的IP地址为61.159.62.129，子网掩码为255.255.255.248，可用于转换的IP地址范围为61.159.62.130～61.159.62.134。要求将内部网址192.168.0.2～192.168.0.6分别转换为合法IP地址61.159.62.130～61.159.62.134。

```
第一步，设置外部端口。
interface serial 0
ip address 61.159.62.129 255.255.255.248
ip nat outside
第二步，设置内部端口。
interface ethernet 0
ip address 192.168.0.1 255.255.255.0
ip nat inside
第三步，在内部本地与外部合法地址之间建立静态地址转换。
ip nat inside source static 内部本地地址 外部合法地址
示例：ip nat inside source static 192.168.0.2 61.159.62.130
//将内部网络地址192.168.0.2转换为合法IP地址61.159.62.130
```

至此，静态地址转换配置完毕。

1.2　运维实例：莫名奇妙的IP地址冲突

网络运维师在工作中遇到的网络问题，故障现象都是千变万化、多种多样的。所以也不能用单一、固定的方法或知识去解决它们，必须根据实际的故障现象，结合自己的工作经验，运用多种方法和知识灵活地排除故障。下面就是自己在实际工作中碰到的一则故障实例，通过对故障现象的分析和故障的排除过程来说明排除网络故障并不是一件简简单单的事情。

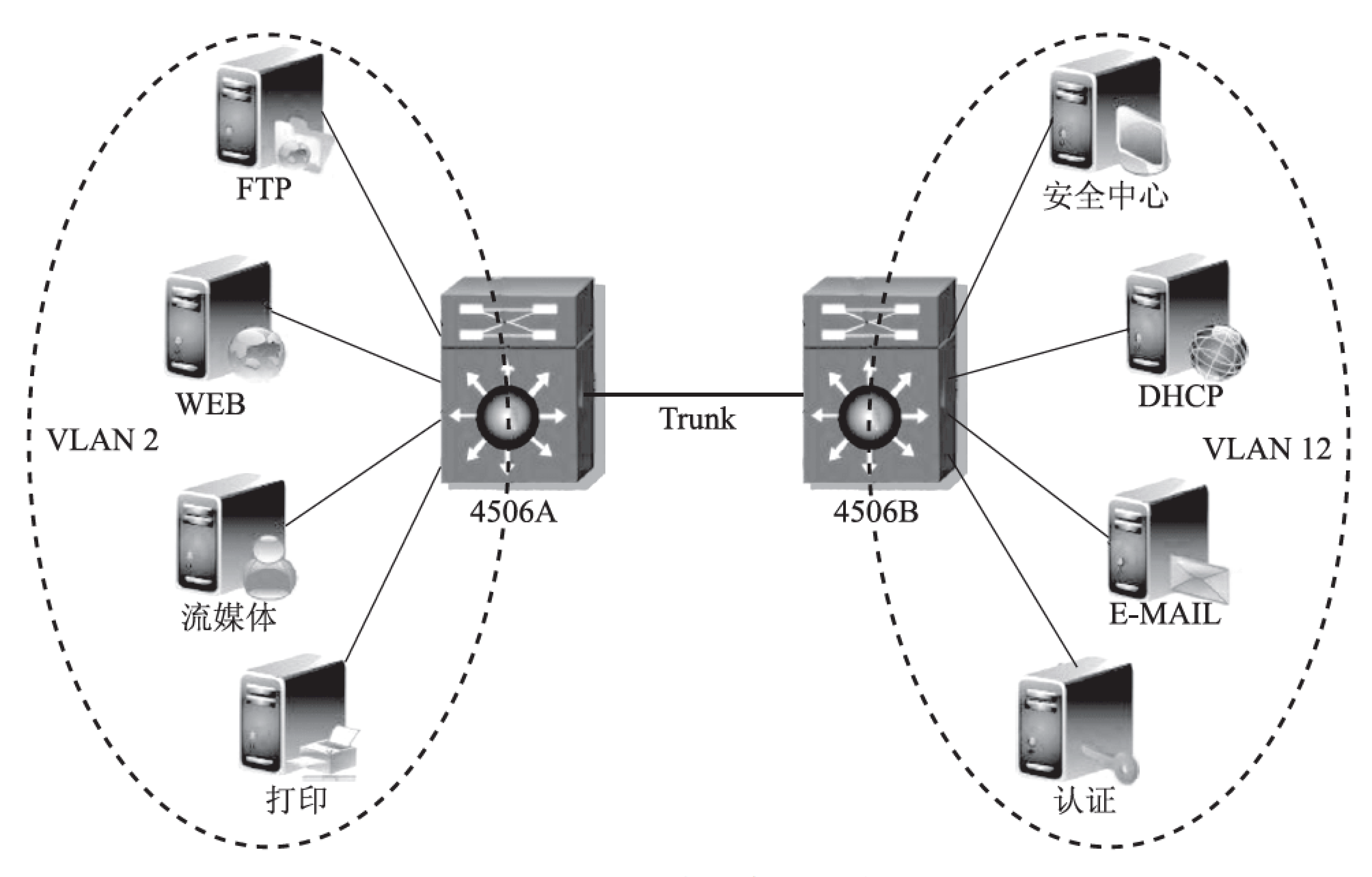


图1-1　公司网络服务器部署图

1. 公司网络服务器部署架构

网络中的服务器部署结构图，如图1-1所示。为了确保重要设备的稳定性和冗余性，核心层交换机使用两台Cisco4506，通过Trunk线连接。在核心交换机上连接有单位重要的服务器，如安全中心、DHCP、E-MAIL和WEB服务器等。单位IP地址的部署，使用的是B类私有172网段的地址。其中，连接在Cisco4506A上的FTP服务器、WEB服务器和流媒体服务器都是戴尔牌的，打印服务器是IBM

的。连接在Cisco4506B上的安全中心服务器和DHCP服务器是戴尔的，E-MAIL服务器是HP的，认证服务器是IBM的。

两台Cisco4506之间的连接情况及Cisco4506A和服务器间的连接情况如下所示：

```
    Cisco4506A GigabitEthernet 1/1 <----> Cisco4506B GigabitEthernet 1/1
    Cisco4506A GigabitEthernet 4/1 <----> FTP Server Eth0
    Cisco4506A GigabitEthernet 4/2 <----> Web Server Eth0
    Cisco4506A GigabitEthernet 4/3 <----> 流媒体服务器Eth0
    Cisco4506A GigabitEthernet 4/4 <----> 打印服务器 Eth0
```

Cisco4506B和服务器之间的连接情况如下所示：

```
    Cisco4506B GigabitEthernet 4/1 <----> 安全中心服务器 Eth0
    Cisco4506B GigabitEthernet 4/2 <----> DHCP Server Eth0
    Cisco4506B GigabitEthernet 4/3 <----> E-Mail Server Eth0
    Cisco4506B GigabitEthernet 4/4 <----> 认证服务器 Eth0
```

2. 核心交换机的网络配置情况

Cisco4506A上的配置如下所示：

```
    Cisco4506A#VLAN database
    Cisco4506A(VLAN)#VLAN 2
```

```
Cisco4506A(VLAN)#apply
Cisco4506A (config)#interface range gigabitEthernet 4/1-4
Cisco4506A (config-if-range)# switchport
Cisco4506A (config-if-range)#switchport access VLAN 2
Cisco4506A(config)#int VLAN 2
Cisco4506A(config-if)#ip address 172.16.2.252 255.255.255.0
//创建VLAN 2的SVI接口，并指定IP地址
Cisco4506A(config-if)#no shutdown
Cisco4506A(config-if)standby 2 priority 250 preempt
Cisco4506A(config-if)standby 2 ip 172.16.2.254
//配置VLAN 2的HSRP参数
Cisco4506A(config)#int VLAN 12
Cisco4506A(config-if)#ip address 172.16.12.252 255.255.255.0
Cisco4506A(config-if)#no shutdown
Cisco4506A(config-if)standby 12 priority 250 preempt
Cisco4506A(config-if)standby 12 ip 172.16.12.254
```

命令“standby 2 priority 250 preempt”中的“priority”是配置HSRP的优先级，2为组序号，它的取值范围为0～255，250为优先级的值，取值范围为0～255，数值越大优先级越高。

优先级将决定一台路由器在HSRP备份组中的状态，优先级最高的路由器将成为活动路由器，其他优先级低的路由器将成为备用路由器。当活动路由器失效后，备用路由器将替代它成为活动路由器。当活动和备用路由器都失效后，其他路由器将参与活动和备用路由器的选举工作。优先级都相同时，接口IP地址高的将成为活动路由器。

“preempt”是配置HSRP为抢占模式。如果需要高优先级的路由器能主动抢

占成为活动路由器，则要配置此命令。配置preempt后，能够保证优先级高的路由器失效恢复后总能成为活动路由器。活动路由器失效后，优先级最高的备用路由器将处于活动状态，如果没有使用preempt技术，则当活动路由器恢复后，它只能处于备用状态，先前的备用路由器代替其角色处于活动状态。

Cisco4506B上的配置如下所示：

```
Cisco4506B#VLAN database
Cisco4506B(VLAN)#VLAN 12
Cisco4506B(VLAN)#apply
Cisco4506B (config)#interface range gigabitEthernet 4/1 -4
Cisco4506B (config-if-range)# switchport
Cisco4506B (config-if-range)#switchport access VLAN 12

Cisco4506B(config)#int VLAN 12
Cisco4506B(config-if)#ip address 172.16.12.253 255.255.255.0
Cisco4506B(config-if)#no shutdown
Cisco4506B(config-if)standby 12 priority 249 preempt
Cisco4506B(config-if)standby 12 ip 172.16.12.254

Cisco4506B(config)#int VLAN 2
Cisco4506B(config-if)#ip address 172.16.2.253 255.255.255.0
Cisco4506B(config-if)#no shutdown
Cisco4506B(config-if)standby 2 priority 249 preempt
Cisco4506B(config-if)standby 2 ip 172.16.2.254
```

3. 问题的发生和主要的故障现象

在公司的网络中，还部署有入侵检测系统IDS和入侵防御系统IPS，在图1-1所示的“安全中心”服务器的浏览器中，分别输入IDS和IPS的管理IP地址后，就可以对这两个安全设备进行管理和设置，也可以查看这两个安全设备上的一些日志和报警信息。这也就是在远程通过浏览器，用WEB的方式对安全设备进行远程管理和监控。网络中的IDS设备是连接到Cisco4506A的GigabitEthernet 3/1镜像端口上，在4506A上相关的配置命令如下所示：

```
Cisco4506A (config)#monitor session 1 source VLAN 2 , 12 both
Cisco4506A (config)#monitor session 1 destination interface gigabitEthernet 3/1
```

在“安全中心”服务器上，通过IDS设备对图1-1中，VLAN 2和VLAN 12两个区域的监控，IDS总会提示IP地址192.168.0.120冲突的告警信息。也就是说在图1-1中的VLAN 2、VLAN 12中存在两个设备都在使用IP地址192.168.0.120。因为从上面4506A上的两行配置命令可以看出IDS只监控了VLAN 2和VLAN 12两个网段的数据。

刚看到告警信息时觉得很奇怪，因为公司的网络中使用的都是172网段的地址，根本就没有部署过192的地址，所以首先想到的是是不是有攻击。而且IDS设备能够显示出引起IP地址冲突的两个MAC地址：842b.2b48.a187和842b.2b58.ea6f。

4. 排除故障的步骤

(1)因为IDS监控的是VLAN 2和VLAN 12两个网段，所以就首先要排除冲突是发生在VLAN 2，还是发生在VLAN 12中。把在4506A上的配置“Cisco4506A (config)#monitor session 1 source VLAN 2，12 both”改为“Cisco4506A (config)#monitor session 1 source VLAN 2 both”，也就是只让IDS监控VLAN 2中的数据。结果发现IDS还是会提示IP地址192.168.0.120冲突的告警信息。

接着，把配置“Cisco4506A (config)#monitor session 1 source VLAN 2 both”改为“Cisco4506A (config)#monitor session 1 source VLAN 12 both”，也就是只让

IDS监控VLAN 12中的数据。但IDS依旧会提示IP地址192.168.0.120冲突。所以说目前在VLAN 2和VLAN 12中都存在IP地址192.168.0.120冲突的问题。难道说攻击都已经渗透到网络核心层的这两个VLAN中了？

(2)因为在IDS上还提示了引起IP地址冲突的两个MAC地址，而MAC地址具有全球唯一性，所以可以通过这两个MAC地址找到IP地址192.168.0.120是和什么设备关联在一起的。所以，在Cisco4506A上执行以下命令：

```
Cisco4506A#sh mac address-table | include 842b.2b
  2    842b.2b48.a187    DYNAMIC      Gi4/1
  2    842b.2b58.ea6f    DYNAMIC      Gi4/2
```

从以上命令的输出结果，可以看出在VLAN 2中引起IP地址192.168.0.120冲突的两个设备，就是连接在Cisco4506A端口Gi4/1上的FTP Server和连接在Cisco4506A端口Gi4/2上的Web Server。但是在进行网络部署时，并没有在这两个服务器上配置192的IP地址。为了更加确认这种判断，还在FTP和Web服务器上的“命令行”中执行了命令“ifconfig-a”，从输出的结果中也没有看到192网段的IP地址，都是172的地址。

因为从上面的第“(1)”点中可以看出，在VLAN 12中也存在IP地址192.168.0.120冲突的问题。所以，在Cisco4506B上也执行了“Cisco4506B#sh mac address-table”命令，结果发现引起IP地址冲突的两个设备是连接在Cisco4506B端口Gi4/1上的安全中心服务器和连接在Cisco4506B端口Gi4/2上的DHCP Server。但是，我们在这两个服务器上也没有配置192网段的地址。

(3)综合上面排查故障的过程，可以发现引起IP地址冲突的服务器都是DELL服务器。因为确实查找不到引起IP地址冲突的原因，就在百度中搜索了“戴尔192.168.0.120冲突”相关信息，发现192.168.0.120这个IP地址是戴尔服务器远程控制功能中默认使用的一个IP地址。戴尔服务器的远程控制功能是通过DRAC(Dell Remote Access Controller，戴尔远程控制卡)实现的，它是一种系统管理硬件和软件解决方案，专门用于为 Dell PowerEdge系统提供远程管理功能、崩溃系统恢复和电源控制功能。

也就是用户在远程若能访问到图1-1中VLAN 2或VLAN 12中的192.168.0.120这个IP地址，也就能实现在远程对VLAN 2或VLAN 12中的戴尔服务器进行简单的管理和配置。因为默认情况下具备DRAC功能的戴尔服务器，都在远程控制卡上配置了192.168.0.120这个IP地址，而且DRAC功能的实现是通过共用戴尔服务器的网口实现的。

所以，连接在Cisco4506A上的，都位于VLAN 2中的戴尔牌FTP服务器、Web服务器和流媒体服务器，在它们连接到4506A上的网口上都同时具备了两个IP地址，一个是172网段的地址，一个是192.168.0.120地址。而且，它们都位于同一个VLAN中，所以IDS在监控时就会发出IP地址冲突的告警信息。同样道理，连接在Cisco4506B上的安全中心服务器和DHCP服务器也会出现同样的地址冲突告警。

5. 总结

(1)为了验证戴尔服务器的DRAC功能，在图1-1的VLAN 2中接入一台笔记本电脑，电脑上的IP地址配置为192.168.0.144，子网掩码为255.255.255.0，如图1-2所示。

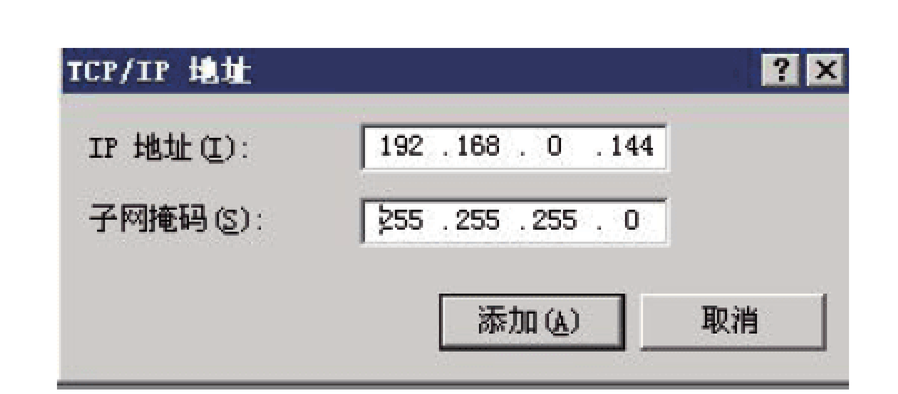


图1-2 笔记本电脑网络配置参数

然后，在笔记本电脑的浏览器中输入网址“https://192.168.0.120”后回车，就可以看到如图1-3所示的登录界面，输入默认的用户名root，密码calvin后就可以进入到戴尔服务器的Web管理控制界面。



图1-3 通过DRAC管理戴尔服务器的登录界面

在管理界面中可以看到戴尔服务器的基本配置属性，还可以对“电源”和“警报”进行管理配置，也可以浏览查看服务器的日志信息。而且在“属性”的系统摘要中，可以看到服务器的IP地址信息，其中也包括有192.168.0.120这个IP地址，如图1-4所示。



图1-4　通过DRAC管理戴尔服务器的系统摘要信息

(2)要解决在IDS设备中总提示192.168.0.120冲突的告警信息，可以使用两种解决办法。一是重新启动戴尔服务器，进入到服务器的CMOS设置，在其中把“远程控制卡”的功能关闭即可。二是进入到服务器的CMOS中，对DRAC卡的IP地址进行设置，可以把图1-1中位于VLAN 2或VLAN 12中的几台戴尔服务器的IP地址设置成相互间不一样的地址，也可以把它们配置成为172网段的IP地址，这样就可以通过公司的网络，远程对各个戴尔服务器进行简单的管理和配置。如图1-5所示，是在CMOS中设置DRAC卡IP地址的界面。

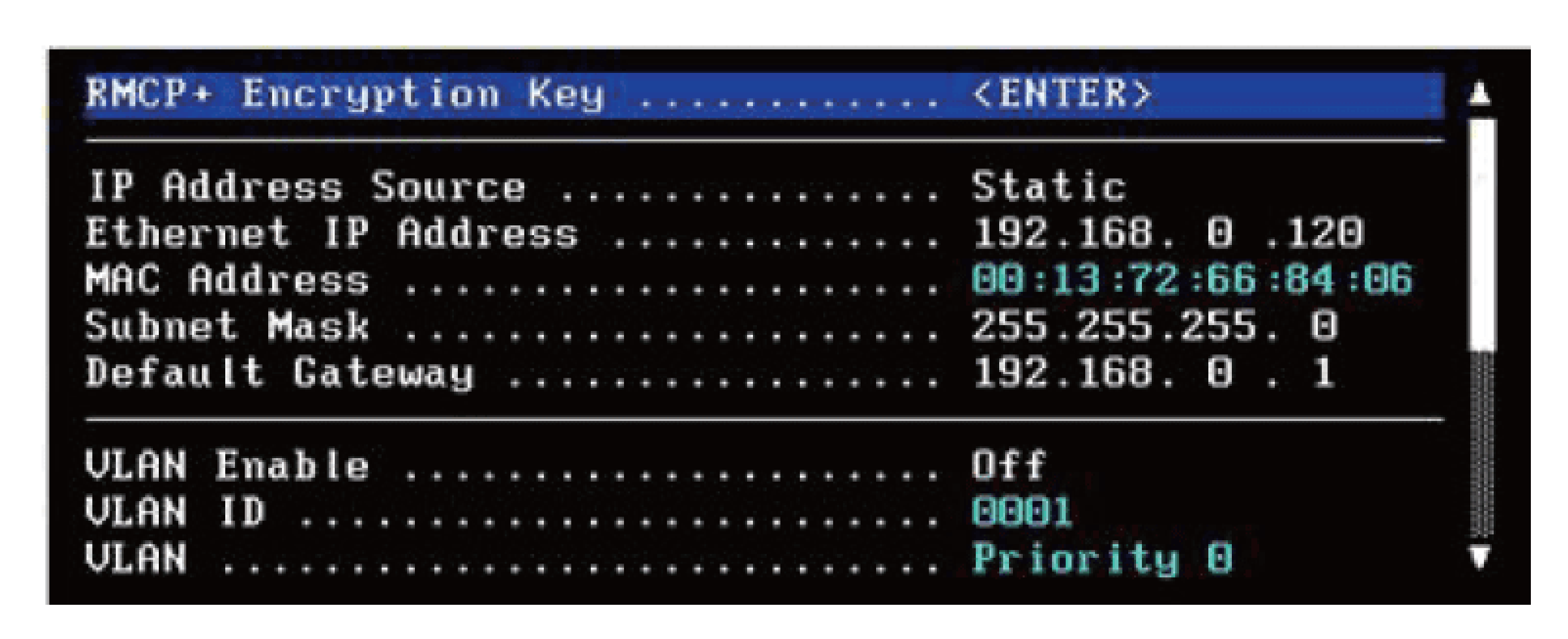


图1-5　在戴尔服务器CMOS中设置DRAC卡IP地址

1.3　运维实例：双网卡在网络中的实际应用

因为用户的特殊需求，要保证其上互联网的高可靠性，所以考虑到在他的电脑上使用两块网卡访问互联网。这样当其中一块网卡故障或者是连接在网卡上的线路故障，另一块网卡和线路还可以继续保证用户正常地使用Internet。另外，还有一种方案就是使用双网卡绑定软件，把两个网卡绑定虚拟成一块网卡，但是这种方案就要多使用一个软件，这无疑就多增加了一个故障点。若用户在使用中，绑定双网卡的软件发生故障，也会影响到用户正常访问互联网。那么在不使用双网卡绑定软件的情况下，能不能把PC上的两块网卡同时接入到网络中？当其中的一块网卡故障后，另一块网卡是不是同样可以保证用户对互联网的正常使用？经过测试是可以的，以下是实验的过程。

1. 网络结构图

(1)网络设备间的主要连接情况。网络结构图如图1-6所示。为了确保重要设备的稳定性和冗余性，核心层交换机使用两台Cisco4506，通过Trunk线连接。在接入层使用了多台Cisco3750交换机，图示为了简洁，只画出了两台。在核心交换机上连接有单位重要的服务器，如DHCP、E-MAIL服务器、WEB服务器等。其中，DHCP服务器在图1-6中只画出了一台，现实中存在两台双机热备的DHCP服务器。同样，对于连接到Internet的光纤，也有两条，这都是为了保障整个网络的高可靠性。IP地址的部署，使用的是C类私有192网段的地址。DHCP服务器的IP地址为192.168.1.1。Cisco4506和Cisco3750之间也是Trunk连接。图1-6部署模式设备间的连接情况如下所示：

```
    Cisco4506A GigabitEthernet1/1 <----> Cisco4506B GigabitEthernet1/1

    Cisco4506A GigabitEthernet2/1 <----> Cisco3750A GigabitEthernet1/0/28
```

```
    Cisco4506B GigabitEthernet2/1 <----> Cisco3750B
GigabitEthernet1/0/28
    Cisco3750A GigabitEthernet1/0/25 <----> Cisco3750B
GigabitEthernet1/0/25
```

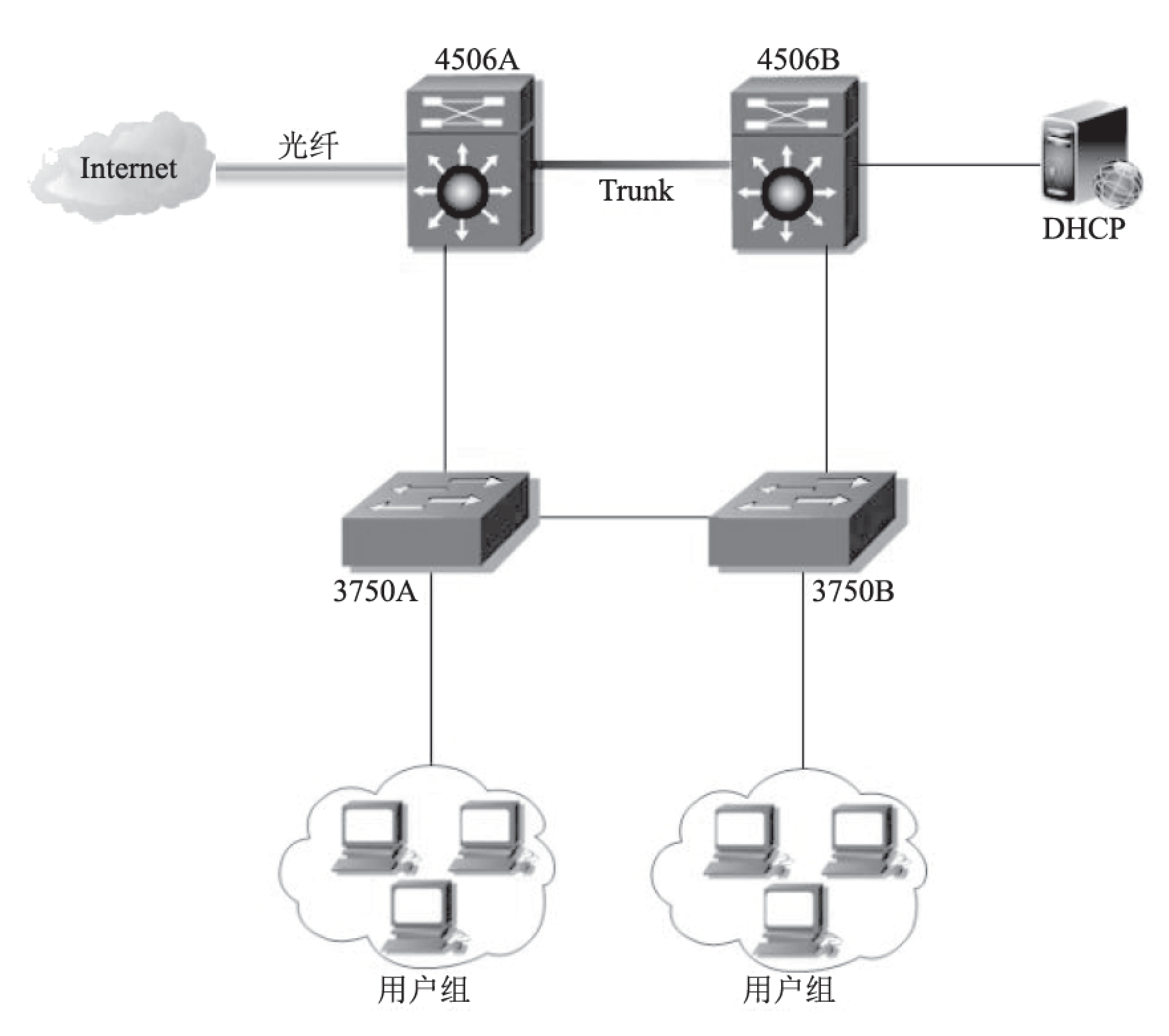


图1-6 单位网络结构图

(2)在Cisco4506A和Cisco4506B上的主要配置。在图1-6的连接中，Cisco4506A和Cisco4506B之间的连接、Cisco4506和Cisco3750之间的连接及Cisco3750A和Cisco3750B之间的连接都是通过光纤连接的。而其他的连接使用的都是双绞线的连接。在Cisco4506A上的主要配置，如下所示：

```
    hostname Cisco4506A
    !
    interface GigabitEthernet1/1
```

```
 description Link4506B_1/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 201,220
 switchport mode trunk
!
interface GigabitEthernet2/1
 description Link3750A
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 201,220
 switchport mode trunk
!
interface VLAN 201
 ip address 192.168.201.252  255.255.255.0
standby 201 ip 192.168.201.254
standby 201 priority 120
standby 201 preempt
!
interface VLAN 220
 ip address 192.168.220.252  255.255.255.0
standby 220 ip 192.168.220.254
 standby 220 priority 120
standby 220 preempt
```

其中命令“ip address 192.168.201.252 255.255.255.0”是给指定的VLAN配置

IP地址。

命令“standby 201 priority 120”中的“priority”是配置HSRP的优先级，201为组序号，它的取值范围为0～255，120为优先级的值，取值范围为0～255，数值越大优先级越高。

优先级将决定一台路由器在HSRP备份组中的状态，优先级最高的路由器将成为活动路由器，其他优先级低的路由器将成为备用路由器。当活动路由器失效后，备用路由器将替代它成为活动路由器。当活动和备用路由器都失效后，其他路由器将参与活动和备用路由器的选举工作。优先级都相同时，接口IP地址高的将成为活动路由器。

“preempt”是配置HSRP为抢占模式。如果需要高优先级的路由器能主动抢占成为活动路由器，则要配置此命令。配置preempt后，能够保证优先级高的路由器失效恢复后总能成为活动路由器。活动路由器失效后，优先级最高的备用路由器将处于活动状态，如果没有使用preempt技术，则当活动路由器恢复后，它只能处于备用状态，先前的备用路由器代替其角色处于活动状态。

命令“standby 201 ip 192.168.201.254”作用是启动HSRP，如果虚拟IP地址不指定，路由器就不会参与备份。虚拟IP应该是接口所在的网段内的地址，不能配置为接口上的IP地址。

在Cisco4506B上的主要配置如下所示：

```
hostname Cisco4506B
!
interface GigabitEthernet1/1
 description Link4506A_1/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 201,220
 switchport mode trunk
!
```

```
interface GigabitEthernet2/1
 description Link3750B
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 201,220
 switchport mode trunk
!
interface VLAN 201
ip address 192.168.201.253  255.255.255.0
standby 201 ip 192.168.201.254
 standby 201 priority 110
standby 201 preempt
!
interface VLAN 220
ip address 192.168.220.253  255.255.255.0
standby 220 ip 192.168.220.254
 standby 220 priority 110
standby 220 preempt
```

(3)在Cisco3750A和Cisco3750B上的主要配置如下所示：

```
hostname Cisco3750A
!
interface GigabitEthernet1/0/25
 description Link3750B_1/0/25
 switchport trunk encapsulation dot1q
```

```
 switchport trunk allowed VLAN 201,220
 switchport mode trunk
!
interface GigabitEthernet1/0/28
 description Link4506A
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 201,220
 switchport mode trunk
```

在Cisco3750B上的主要配置如下所示：

```
hostname Cisco3750B
!
interface GigabitEthernet1/0/25
 description Link3750A_1/0/25
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 201,220
 switchport mode trunk
!
interface GigabitEthernet1/0/28
 description Link4506B
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 201,220
 switchport mode trunk
```

2. PC上两块网卡的IP地址位于不同的VLAN中

如图1-7所示，电脑PC上有两块网卡，分别用网线连接到Cisco3750上。其中，PC上左边的网卡通过网线连接到3750的VLAN 201中，右边的网卡通过网线连接到3750的VLAN 220中。因为从图1-6中可以看出，网络中配置有DHCP服务器，所以当PC加电，启动操作系统后，电脑会从DHCP服务器上自动获取IP地址。这样两个网卡都能从DHCP服务器上分别获取到一个IP地址，也就是同一个操作系统中会有两个IP地址同时处于活动状态。下面阴影部分内容是在电脑的“命令提示符CMD”中执行命令“ipconfig /all”后的显示结果，其中电脑PC上使用的操作系统是“Win 7旗舰版”。

```
C:\Users\Administrator>ipconfig /all
以太网适配器 本地连接 2:
描述...............: Realtek RTL8139 Family Fast Ethernet NIC
物理地址...............: 00-1A-EB-4D-07-4A
DHCP 已启用...............: 是
自动配置已启用...............: 是
IPv4 地址...............: 192.168.201.35(首选)
子网掩码...............: 255.255.255.0
获得租约的时间...............: 2012年1月19日 15:42:38
租约过期的时间...............: 2012年3月19日 15:42:38
默认网关...............: 192.168.201.254
DHCP 服务器...............: 192.168.1.1
DNS 服务器...............: 85.61.14.251
                          8.8.8.8
以太网适配器 本地连接:
```

```
    描述...............: Intel(R)82566DM-2 Gigabit Network
Connection
    物理地址...............: 00-31-86-14-16-A2
    DHCP 已启用...............: 是
    自动配置已启用...............: 是
    IPv4 地址...............: 192.168.220.5(首选)
    子网掩码...............: 255.255.255.0
    获得租约的时间...............: 2012年1月19日 15:47:09
    租约过期的时间...............: 2012年3月19日 15:47:09
    默认网关...............: 192.168.220.254
    DHCP 服务器...............: 192.168.1.1
    DNS 服务器...............: 85.61.14.251
                              8.8.8.8
```

从上面的输出结果可以看出，Win 7操作系统中共有两个网络连接，“本地连接 2”和“本地连接”，前者的IP地址为192.168.201.35，也就是连接到Cisco3750中VLAN 201上的那个网卡的IP地址；后者的IP地址为192.168.220.5，也就是连接到Cisco3750中VLAN 220上的那个网卡的IP 地址。两个网卡的默认网关地址都是从DHCP服务器上自动获取的，前者是192.168.201.254，后者是192.168.220.254。两个网卡从DHCP服务器上自动获取的DNS的地址都是一样的，为85.61.14.251和8.8.8.8。从上面的输出中也可以看出网络中DHCP服务器的IP地址为192.168.1.1。两个网卡自动获取的IP地址都有“获得租约的时间”和“租约过期的时间”，而且也能显示出两个网卡的MAC地址分别为“00-1A-EB-4D-07-4A”和“00-31-86-14-16-A2”。

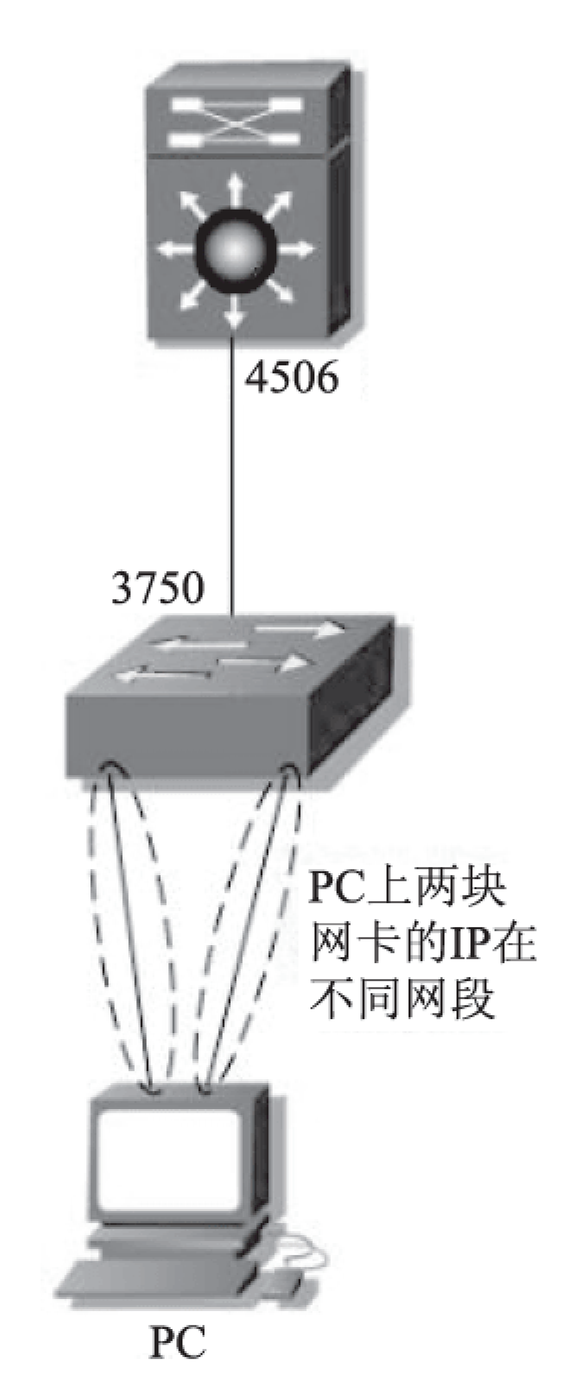


图1-7　PC上两块网卡位于不同的VLAN中

现在，PC上同时有两个正常活动的IP地址，那Win 7系统能不能正常访问互联网？若是能正常访问的话，出去的数据是从哪个网卡出去的？从互联网上返回电脑PC上的数据又是从哪个网卡传输到电脑上？是通过“本地连接 2”的网卡，还是通过“本地连接”的网卡？

经过测试，发现在PC上可以正常访问互联网上所有的数据。和在电脑上安装一块网卡访问互联网的效果是一样的。也就是，同时使用两块网卡并不影响用户对网络的正常访问。下面是在电脑PC上执行命令“ping www.baidu.com”的输出结果：

```
C:\Users\Administrator>ping www.baidu.com
正在 Ping www.a.shifen.com [61.135.169.125] 具有 32 字节的数据：
来自 61.135.169.125 的回复：字节=32 时间=2ms TTL=50
来自 61.135.169.125 的回复：字节=32 时间=2ms TTL=50
```

```
来自 61.135.169.125 的回复：字节=32 时间=2ms TTL=50
来自 61.135.169.125 的回复：字节=32 时间=2ms TTL=50
61.135.169.125 的 Ping 统计信息：
    数据包：已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位)：
    最短 = 2ms，最长 = 2ms，平均 = 2ms
```

但是从上面的输出结果也看不出，电脑的哪个网卡在和外界的互联网进行通信。后来想到，其实每一台具有三层IP地址的网络设备，在本质上它就相当于一台路由器，其中都包括有路由表。这些设备在发出数据包时都会对照自己的路由表，来决定到底是从哪个接口上把数据包发送出去。所以在图1-7中的PC上肯定也存在路由表。下面阴影部分内容是在电脑的“命令提示符CMD”中执行命令“route print”后的显示结果：

```
C:\Users\Administrator>route print
============================
接口列表
 13...00 1a eb 4d 07 4a ......Realtek RTL8139 Family Fast Ethernet NIC
 12...00 31 86 14 16 a2 ......Intel(R)82566DM-2 Gigabit Network Connection
============================
IPv4 路由表
============================
```

```
活动路由：
网络目标    网络掩码       网关            接口            跃点数
0.0.0.0     0.0.0.0     192.168.201.254  192.168.201.35   20
0.0.0.0    0.0.0.0    192.168.220.254  192.168.220.5   10
192.168.201.0   255.255.255.0   在链路上 192.168.201.35   276
192.168.201.35   255.255.255.255   在链路上 192.168.201.35   276
192.168.201.255 255.255.255.255 在链路上 192.168.201.35 276
192.168.220.0   255.255.255.0   在链路上 192.168.220.5 266
192.168.220.5   255.255.255.255   在链路上   192.168.220.5   266
192.168.220.255   255.255.255.255   在链路上   192.168.220.5   266
255.255.255.255    255.255.255.255   在链路上   192.168.201.35   276
255.255.255.255   255.255.255.255   在链路上   192.168.220.5   266
= = = = = = = = = = = = = = = = = = = = = = = = = = = = =
```

“route print”命令可以显示出电脑中的路由表情况。从上面输出的“接口列表”中可以看出，PC通过两个接口和外界的互联网进行通信，从两个接口的MAC地址就能知道它们分别对应电脑PC上的“本地连接 2”和“本地连接”的两个网卡。从“IPv4路由表”中可以看出，在电脑PC上存在两个默认网关“192.168.201.254”和“192.168.220.254”。有两个默认网关，那电脑PC到底是使用哪个网关，把它上面的数据发送到互联网上的？其实，在上面的输出结果中还有一个重要的参数——“跃点数”。跃点数越小的路由，就会被选为从电脑上发出数据包的活动路由，也就是说网关“192.168.220.254”最终成为电脑PC和外界通信的活动网关。对照上面命令“ipconfig /all”的输出结果，可以看出是网卡“Intel(R)82566DM-2 Gigabit Network Connection”在和外界进行着数据的交互。

为了进一步验证是不是网卡“Intel(R)82566DM”在和外界进行数据交互，在命令行提示符中执行命令“netstat -an”，以下是输出结果。

```
C:\Users\Administrator>netstat -an
活动连接
  协议   本地地址              外部地址            状态
  TCP    192.168.201.35:139   0.0.0.0:0          LISTENING
  TCP    192.168.220.5:139    0.0.0.0:0          LISTENING
  TCP    192.168.220.5:1808   64.4.44.95:1863    ESTABLISHED
  TCP    192.168.220.5:3904   123.125.114.64:80  ESTABLISHED
  TCP    192.168.220.5:3905   123.125.114.64:80  ESTABLISHED
  TCP    192.168.220.5:3906   123.125.114.17:80  ESTABLISHED
  TCP    192.168.220.5:3907   123.125.115.43:80  ESTABLISHED
```

“netstat -an”命令，可以以数字的形式显示电脑中所有的连接和监听端口。从上面的输出结果可以看出，和外界建立“ESTABLISHED”的都是“192.168.220.5”这个IP地址，而地址“192.168.201.35”一直处于监听状态，并没有与外界建立连接和通信。所以说电脑PC上，连接到Cisco3750的两块网卡中只有“Intel(R)82566DM”这一块网卡和外界进行数据通信。而另一块网卡其实是处于备用状态的，一旦网卡“Intel(R)82566DM”故障，也就是在“route print”命令的输出中，路由“0.0.0.0   0.0.0.0 192.168.220.254 192.168.220.5 10”消失，网卡“Realtek RTL8139”马上就会承担起和互联网进行数据交互的接口。也就是在“route print”命令的输出中，路由“0.0.0.0 0.0.0.0 192.168.201.254 192.168.201.35 20”就会成为活动路由。

从上面的测试结果可以得出这样的结论：“在一台电脑上安装两个网卡，只要这两个网卡在路由表中的，两条默认路由的‘跃点数’不一样，那电脑就会选择‘跃点数’比较小的默认路由作为和外界通信的路由。‘跃点数’较大的路由作为备用路由。”

3. 两块网卡的IP地址位于同一VLAN中

两块网卡位于不同的VLAN中，它们获取到的IP地址不一样，路由表中路由条目的“跃点数”也不一样，这样操作系统就可以选择“跃点数”小的路由作为活动路由。但若是把电脑PC的两块网卡接入到同一个VLAN中，两块网卡还是自动从DHCP上获取IP地址和DNS地址，最终在操作系统的路由表中还是会生成两个默认网关路由，而且两条默认路由的网关地址和跃点数这两个参数都应该是一样的，因为它们都位于同一个VLAN中。如图1-8所示，是把电脑PC上的两块网卡都接入到Cisco3750交换机VLAN 201中的示意图。同样，在电脑PC的“命令提示符CMD”中执行命令“ipconfig”，得到如下的输出结果：

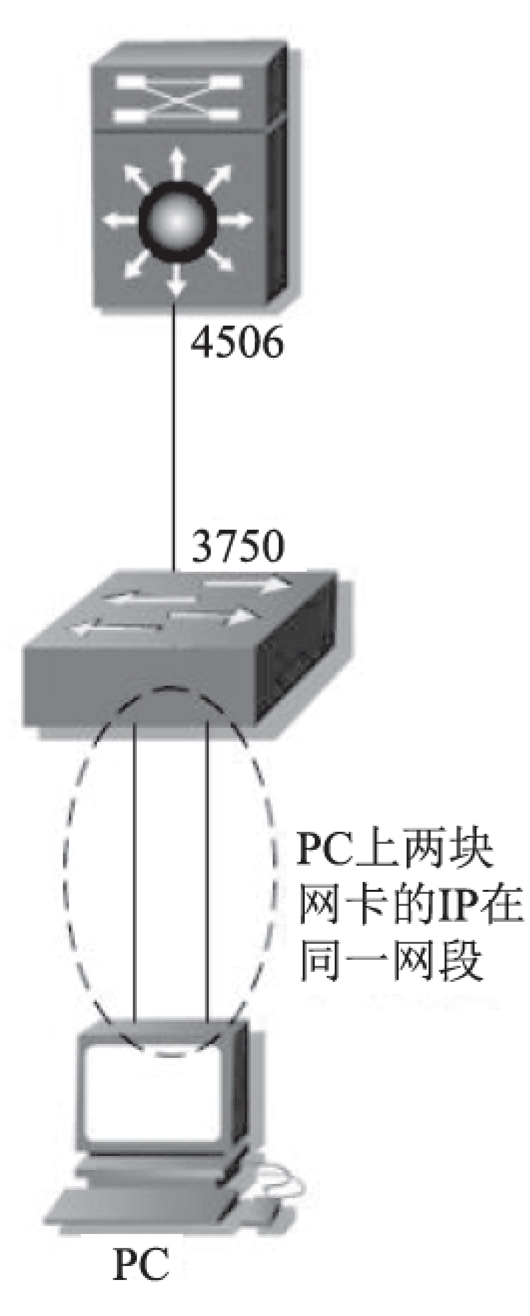


图1-8　PC上两块网卡位于同一个VLAN中

```
C:\Users\Administrator>ipconfig

Windows IP 配置

以太网适配器 本地连接 2:

IPv4 地址...........: 192.168.201.35
```

```
子网掩码............: 255.255.255.0
默认网关............: 192.168.201.254
以太网适配器 本地连接:
IPv4 地址............: 192.168.201.38
子网掩码............: 255.255.255.0
默认网关............: 192.168.201.254
```

从上面的输出中可以看出，“本地连接 2”网卡的IP地址和上面“2”中的没有变化，还是192.168.201.35，但是“本地连接”网卡的IP地址变成了“192.168.201.38”。并且两个网卡的默认网关都是一样的“192.168.201.254”。为了查看电脑PC中的路由表情况，执行命令“route print”，得到如下所示的输出结果：

```
C:\Users\Administrator>route print
= = = = = = = = = = = = = = = = = = = = = = = = = = = = 
IPv4 路由表
= = = = = = = = = = = = = = = = = = = = = = = = = = = = 
活动路由:
网络目标      网络掩码      网关              接口             跃点数
0.0.0.0       0.0.0.0       192.168.201.254   192.168.201.35   20
0.0.0.0       0.0.0.0       192.168.201.254   192.168.201.38   20
192.168.201.0   255.255.255.0   在链路上   192.168.201.35   276
192.168.201.0   255.255.255.0   在链路上   192.168.201.38   276
192.168.201.35   255.255.255.255  在链路上  192.168.201.35   276
192.168.201.38   255.255.255.255  在链路上  192.168.201.38   276
```

```
192.168.201.255  255.255.255.255  在链路上  192.168.201.35  276
192.168.201.255  255.255.255.255  在链路上  192.168.201.38  276
255.255.255.255  255.255.255.255  在链路上  192.168.201.35  276
255.255.255.255  255.255.255.255  在链路上  192.168.201.38  276
= = = = = = = = = = = = = = = = = = = = = = = = = = = = =
```

从上面的输出结果中可以看出，“IPv4路由表”中前两条的默认路由的网关地址变成一样的了，而且跃点数也都成了一样的“20”。那在这种情况下，PC还能不能和外界的互联网保持正常的通信？若是能通信的话，那它使用哪个网卡和外界通信的？

测试在PC上访问百度、新浪等网站，结果一切正常。PC还是能够正常地访问互联网。那PC是使用哪个网卡和外界通信的？经过多次打开互联网上的网页和使用命令“netstat -an”测试，发现PC有时是使用网卡“Intel(R)82566DM”，有时是使用网卡“Realtek RTL8139”和外界进行通信的。也就是在PC中执行命令“netstat -an”后，发现PC有时是使用IP地址“192.168.201.35”和外界建立连接的，有时是使用IP地址“192.168.201.38”进行连接的。

另外，在网络中位于VLAN 220中的一台IP地址是192.168.220.8/24的电脑上，同时执行两个命令“ping 192.168.201.35 -t”和“ping 192.168.201.38 -t”，其中“-t”参数，是指定电脑一直持续不断的执行ping命令。以下是两条命令的输出结果的一部分，因为每一行都是一样的，所以每一个命令就只列出了5行。

```
C:\Users\Administrator>ping 192.168.201.35 -t
正在 Ping 192.168. 201.35 具有 32 字节的数据:
来自 192.168. 201.35 的回复: 字节=32 时间<1ms TTL=64
来自 192.168. 201.35 的回复: 字节=32 时间<1ms TTL=64
来自 192.168. 201.35 的回复: 字节=32 时间<1ms TTL=64
来自 192.168. 201.35 的回复: 字节=32 时间<1ms TTL=64
```

```
来自 192.168. 201.35 的回复: 字节=32 时间<1ms TTL=64
C:\Users\Administrator>ping 192.168.201.38 -t
正在 Ping 192.168. 201.38 具有 32 字节的数据:
来自 192.168. 201.38 的回复: 字节=32 时间<1ms TTL=64
来自 192.168. 201.38 的回复: 字节=32 时间<1ms TTL=64
来自 192.168. 201.38 的回复: 字节=32 时间<1ms TTL=64
来自 192.168. 201.38 的回复: 字节=32 时间<1ms TTL=64
来自 192.168. 201.38 的回复: 字节=32 时间<1ms TTL=64
```

从以上这两个命令的输出结果可以看出，在图1-8中的电脑PC上的两个网卡都“同时”处于正常的活动状态。因为以上两个ping命令是“同时”执行的，并不是执行完其中一个再执行另一个。从上面的测试结果可以得出这样的结论：“在一台电脑上安装两个网卡，即使这两个网卡的‘默认网关’地址和路由表中的‘跃点数’两个参数都一样，也会不影响电脑正常访问互联网。”

4. 两个网卡配置成同一个IP地址

在上面“2”和“3”测试的基础上，再深入一步，就是把两个网卡的IP地址、默认网关和DNS地址全都配置成一样的，看看会出现什么样的结果？电脑是不是还能正常访问互联网？

大家都知道，在XP操作系统中，当网络中存在两个同样的IP地址时，就会在电脑操作系统桌面的右下角，出现一个带感叹号的黄色小三角，并有提示：“IP地址与网络上其他系统有冲突”。但在Win 7操作系统中会出现什么样的情况呢？下面我们就一步一步地测试：

(1)电脑PC上两个网卡的连接示意图和图1-8是一样的，网卡“Intel(R)82566DM”的IP地址、默认网关和DNS地址都是自动从DHCP服务器获得的，分别为“192.168.201.35”、“192.168.201.254”、“85.61.14.251”和“8.8.8.8”。然后，我们把网卡“Realtek RTL8139”的IP地址、默认网关和DNS地址用手工配置，不让它使用从DHCP服务器上获取到的地址，当然网卡

“Realtek RTL8139”还是连接到Cisco3750的VLAN 201中的。配置的参数和网卡“Intel(R)82566DM”的一样。

在电脑PC的“开始”→“控制面板”→“网络和共享中心”→“更改适配器设置”→双击“本地连接”→双击“Internet协议版本4(TCP/IPv4)”，然后在其中配置各项参数，如图1-9所示。

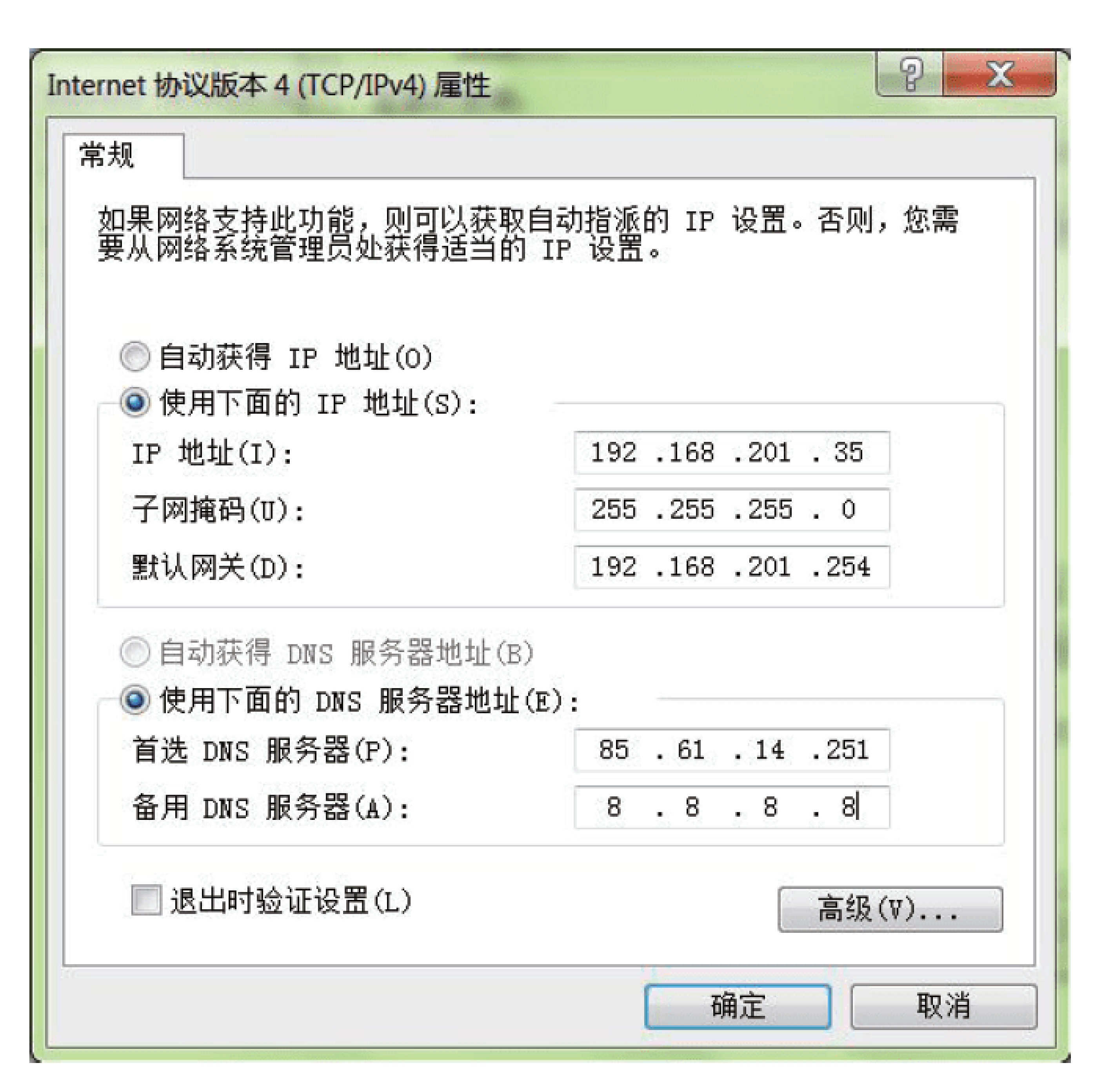


图1-9　手动配置网卡“Realtek RTL8139”参数

(2)在配置完上面的各项参数后，单击图1-9所示的“确定”按钮，会出现如图1-10所示的“警告”对话框。出现这个对话框，就是因为在Win 7系统中，配置了两个一样的IP地址导致的，类似XP系统中提示IP地址冲突一样。不过这种情况下可以不管这些警告，继续单击图1-10所示的“是(Y)”按钮。

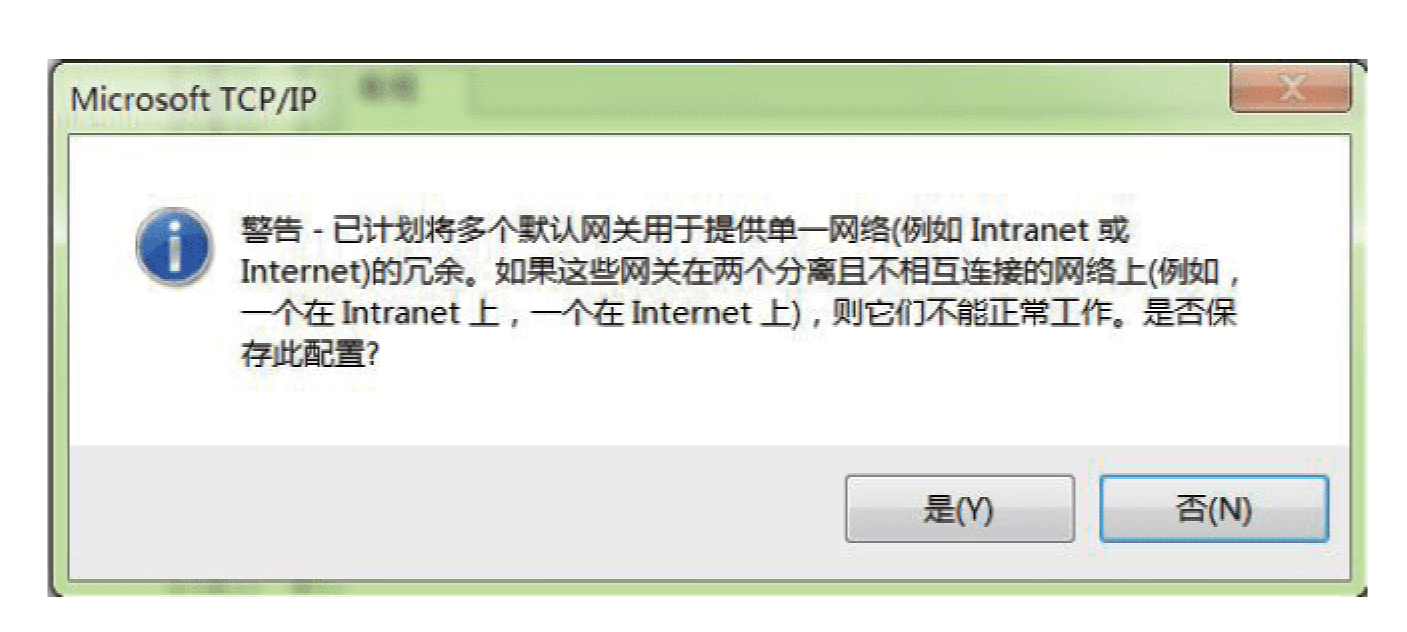


图1-10　Win 7系统弹出的“警告”对话框

(3)进行完上面的配置后，发现图1-8示意图中的电脑PC还是能够正常访问互联网，并没有因为把两个网卡配置都配置成一样的IP地址，而导致访问Internet失败。不过这时Win 7系统还是自动地对电脑PC上两个网卡的网络参数配置作了修改。因为在“(1)”中我们已经把网卡“Realtek RTL8139”的各项网络参数配置成了如图1-9所示的数值，但是到现在的第(3)步，当我们再次打开网卡“Realtek RTL8139”的网络配置参数时，会发现它上面的配置参数变成了如图1-11所示的情况，和图1-9所示的已经有所变化。

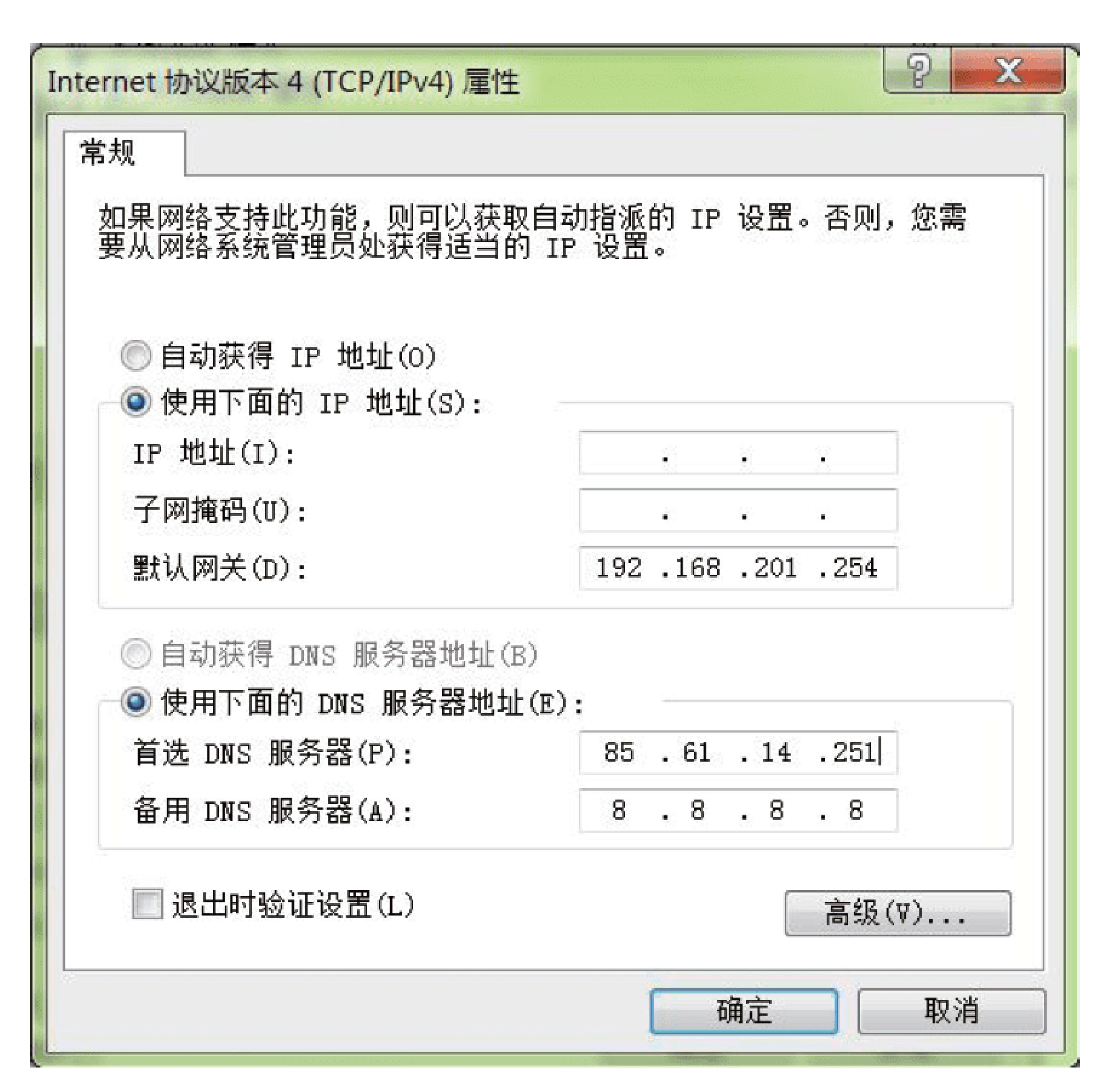


图1-11 网卡“Realtek RTL8139”上的配置参数发生变化

(4)在图1-11中会发现，在图1-9中配置的“IP地址”和“子网掩码”两个参数已经消失了，其他的网络参数到还存在。另外，网卡“Intel(R)82566DM”的IP地址是自动从DHCP服务器上获得的，这时可以查看一下它上面的网络参数会有什么变化？如图1-12所示，是网卡“Intel(R)82566DM”上的参数变化情况。按道理说自动从DHCP服务器上获取各项网络配置参数，是不会在“默认网关(D)”的后面显示出数值的，但现在却把自动获得的“192.168.201.254”的网关地址显示出来了。引起这种变化，还是因为在Win 7系统中把网卡“Realtek RTL8139”的网络参数配置成和网卡“Intel(R)82566DM”一样的。

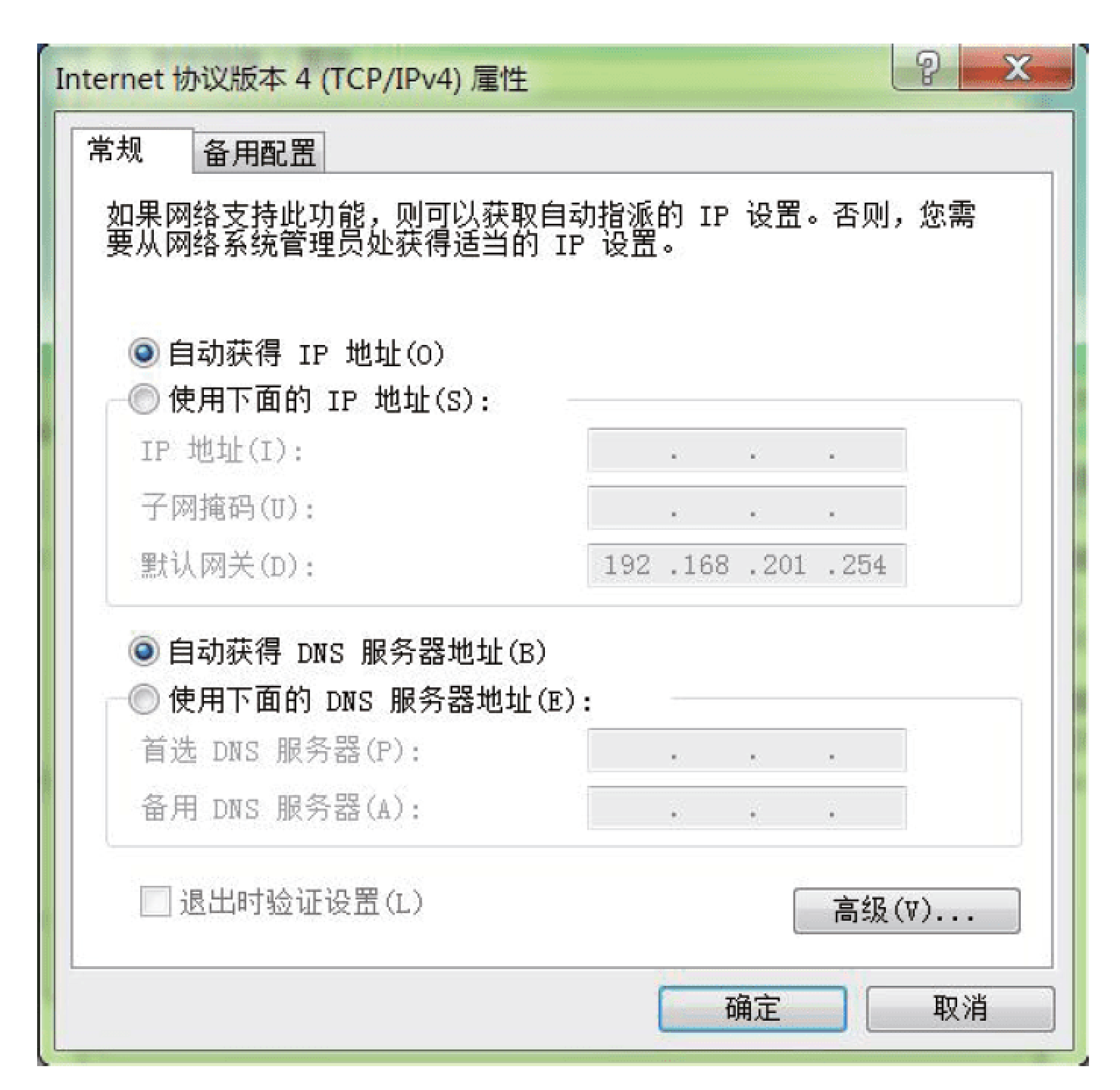


图1-12　网卡“Intel(R) 82566DM”上的网络参数

(5)为了进一步了解清楚两块网卡的网络参数配置情况，就在“命令提示符CMD”中执行了“ipconfig”命令，得到了如下所示的输出结果：

```
C:\Users\Administrator>ipconfig

Windows IP 配置

以太网适配器 本地连接 2:

IPv4 地址............: 192.168.201.35

子网掩码............: 255.255.255.0

默认网关............: 192.168.201.254

以太网适配器 本地连接:

自动配置 IPv4 地址.......: 169.254.54.175

子网掩码............: 255.255.0.0

 默认网关............: 192.168.201.254
```

从上面的输出可以看出网卡“Realtek RTL8139”对应的就是“本地连接”，在上面“(1)”中对其手工配置的IPv4地址和子网掩码“192.168.201.35”“255.255.255.0”，已变成了上面的“169.254.54.175”“255.255.0.0”。所以，这时电脑PC是使用“本地连接 2”的网卡“Intel(R)82566DM”和外界进行通信的。另外，在电脑PC中执行“route print”命令，会得到如下所示的输出结果：

```
IPv4 路由表
= = = = = = = = = = = = = = = = = = = = = = = = = = = = =
活动路由：
网络目标    网络掩码   网关              接口              跃点数
0.0.0.0    0.0.0.0    192.168.201.254   192.168.201.35    20
0.0.0.0    0.0.0.0    192.168.201.254   169.254.245.211   266
= = = = = = = = = = = = = = = = = = = = = = = = = = = = =
```

输出中的“IPv4 路由表”包括两条默认路由，很明显第一条的“跃点数”比第二条要小的多，所以PC还是选择第一条作为它和外界通信的默认路由。第二条路由中的“接口”地址成为了“169.254.245.211”，所以即使第一条默认路由不能使用，PC也不能使用第二条路由和外界进行通信。也就是一旦网卡“Intel(R)82566DM”故障，电脑PC将不能访问Internet。网卡“Realtek RTL8139”也没有起到提高PC访问互联网的高可靠性。

从上面的测试步骤可以得出这样的结论：“在Win 7系统中，当把两块网卡的IP地址配置成一样时，系统会自动对两个网卡的网络参数配置进行调整，以保证操作系统和外界网络的正常通信。”

5. 总结

(1)经过上面的分析，为了提高用户访问网络的高可靠性，可以按照图1-7和图1-8的网络示意图，在用户的电脑上安装配置两块网卡即可。一块网卡故障，另一块网卡还可以继续担负起访问互联网的任务。但图1-7和图1-8的连接示意图

只是测试时使用的方案。在实际的部署中，PC上两个网卡要分别连接在不同的Cisco3750上，这样即使其中的一台3750故障，也不影响PC访问Internet。

(2)提高终端用户访问网络的可靠性，还有一种解决方案就是使用双网卡绑定软件。但这些软件的使用，无疑也增加了故障发生的概率。若是双网卡绑定的软件出现了问题，同样也会导致用户不能访问网络。所以，在普通用户的电脑上，直接安装两块网卡，不使用双网卡绑定软件，是提高电脑访问网络的高可靠性比较好的方案。

但如果是服务器的话，建议还是使用双网卡绑定软件的方案。因为在网络中服务器和普通PC最大的不同就是，服务器上的上行流量比较大，更多的是把服务器上的资源通过网络传送给用户。而对于普通的PC则是网络下行流量比较大，更多的是把网络上的资源下载到PC上。若是在服务器上安装两个网卡，给每个网卡配置一个IP地址，往往会导致很多网络故障。同时也增加了部署应用系统和排除网络方面故障的复杂度。

常用的双网卡绑定软件有NIC Express和Intel的双网卡绑定软件。NIC Express还可以通过绑定多块网卡，达到增加网络带宽的功能。但需要注意的一点就是，在绑定多块网卡时，每一块网卡的传输速率必须相同，这样才可以在网络达到高负荷运行状态时，起到负载均衡的作用。

(3)Windows系统中的Route命令。该命令的主要作用是用来显示、添加和修改Windows系统中的路由表项目。主要包括四种命令：“route print”命令是打印路由；“route add”命令是添加路由；“route delete”命令是删除路由；“route change”命令是修改现有路由。使用不带参数的“route”命令，可以显示相关的帮助信息。

像在上面使用的“route print”命令，就是显示出了PC中当前路由表中使用的路由条目。当在网卡上配置了IP地址后，与IP地址相关的路由条目就会自动地添加到操作系统的路由表中。执行“route print”命令的输出内容中，还包括一个“跃点数”的参数，它的取值范围是1～9999之间的整数，用来在路由表里的多个路由中选择与转发包中的目标地址最为匹配的路由。所选的路由必须具有最小的跃点数。跃点数能够反映出跃点的数量、路径的速度、可靠性、吞吐量及管理属性等。

其实“跃点数”就对应每条路由中的METRIC参数，它可以通过“route change”命令进行修改。当通过“route add”命令添加一条路由时，也会涉及到METRIC参数。例如添加路由的命令“route ADD 157.0.0.0 MASK 255.0.0.0 157.55.80.1 METRIC 3 IF 2”中的“METRIC 3”，就指定了该条路由的跃点数。

导致路由表中某条路由的跃点数比较大的主要原因是，TCP/IP协议是根据每个接口的IP地址、子网掩码和默认网关的配置，自动确定路由表中各路由的跃点数造成的。默认情况下在Windows系统中，“自动跃点”的功能是开启的，它指定了每个接口的速度和路由跃点数。因此最快接口所创建的路由具有最低的跃点数。要关闭“自动跃点”功能，可以在“开始”→“控制面板”→“网络和共享中心”→“更改适配器设置”→双击“本地连接”→双击“Internet协议版本4(TCP/IPv4)”→“高级”。如图1-13所示，在“自动跃点(U)”的前面把勾去掉就可以了。

(4)测试和实验。在上面的步骤中，其实就是一种测试实验。所搭建的网络模型，和在网络设备上所做的各种配置到底能不能正确执行，都是需要经过实实在在的实验才能最终下结论的。任何知识只有经过实践的检验才能最终确定它的正确性！所以，“实践是检验真理的唯一标准”这句话，对于每一个从事网络工作的同志，更应该牢牢铭记！

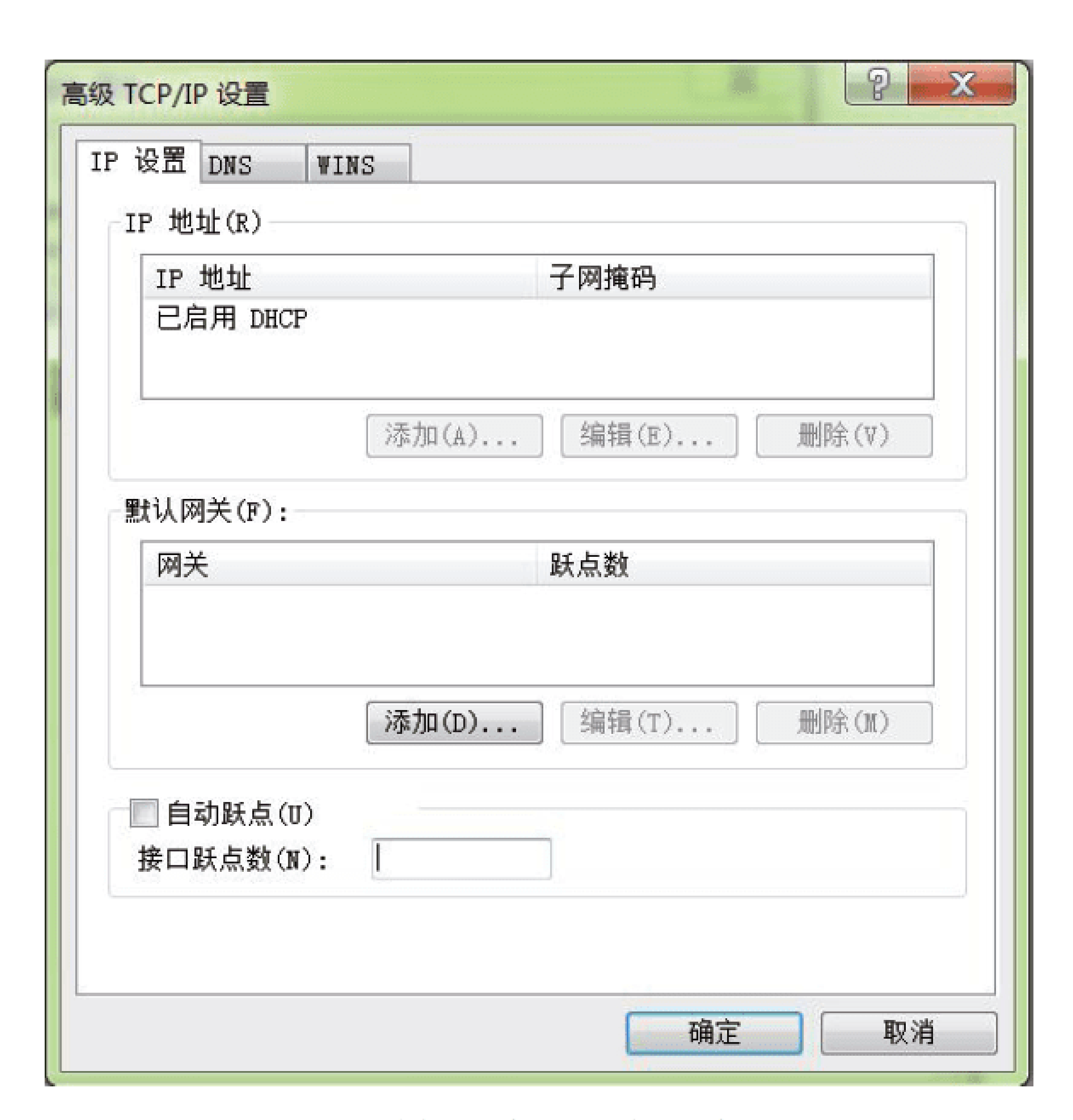


图1-13 关闭“自动跃点”功能图示

包括平时在书本上或网络上看到一些知识点，可能在原理上都能明白，知道它们运行的机制和过程。但即使是这样，也只有通过把这些知识点涉及到的一些命令在交换机、路由器等设备上操作一遍，看看它们到底符合不符合书上所讲的结果。这样心底才能“踏实”地接受这个知识点，因为它经过了实践的检验！

所有从事网络工作者，一定要不断地给自己创造参与实践工作的机会。如果在工作中能接触到现成的网络设备更好，这样学习起来更方便。要是达不到这种条件的话，可以参加一些培训班，它们多多少少都能提供一些操作实验。实在不行，还可以使用一些模拟器，如Dynamips，它们所搭建起来的实验环境也很接近真实的网络环境。总之，一切网络知识，只有经过实践的检验，才能算它是正确的，也才能算自己真正掌握了它。

1.4　运维实例：双IP地址引起的网络故障

网络结构图如图1-14所示，为了确保重要设备的稳定性和冗余性，核心层交换机使用两台Cisco4507，通过Trunk线连接。在接入层使用了多台Cisco3560交换机，图示为了简洁，只画出了两台。在核心交换机上连接有单位重要的服务器，如DHCP、E-MAIL服务器、WEB服务器等。单位IP地址的部署，使用的是C类私有192网段的地址。DHCP服务器的IP地址为192.168.10.1，E-MAIL服务器的IP地址是192.168.3.1。Cisco4507和Cisco3560之间也是Trunk连接。

公司根据部门性质的不同，把它们划入到不同的VLAN中。服务器都位于VLAN 2～VLAN 10中，对应的网络号是192.168.2.0～192.168.10.0，如DHCP服务器位于VLAN 10中，流媒体服务器位于VLAN 2中。服务器的IP地址、默认网关和DNS都是静态配置的。VLAN 11～VLAN 100是属于业务部门使用的，对应的网络号是192.168.11.0～192.168.100.0。VLAN 101～VLAN 200是属于办公部门使用的，对应的网络号是192.168.101.0～192.168.200.0。VLAN号和网络号之间都是对应的。VLAN中的PC都是通过Cisco3560接入到网络中，3560都是二层配置，三层的配置都在Cisco4507上，也就是VLAN间的路由都是通过4507完成的。PC的IP地址、默认网关和DNS都是自动从DHCP服务器上获得的，不用手工静态配置。

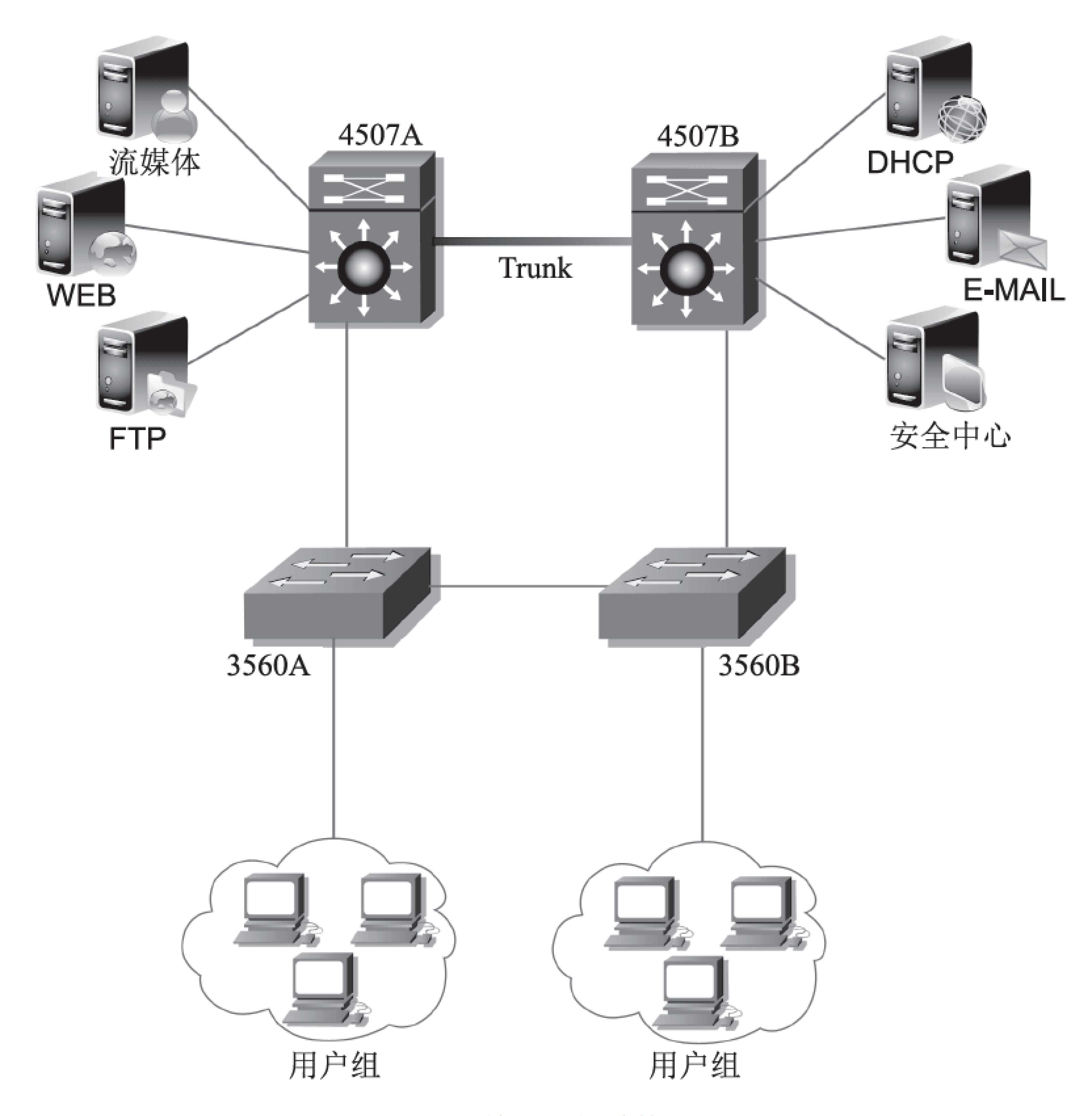


图1-14　单位网络结构图

1. 故障发生的过程

公司流媒体服务器位于VLAN 2中，IP地址为192.168.2.8/24。网络中有权限的用户可以进入到服务器中下载、上传和编辑一些视频剪辑。一天早上，业务网VLAN 12中的很多用户反映它们部门的人员都不能访问流媒体服务器，也不能进入服务器中流媒体应用系统的Web界面。

但是VLAN 12中的用户访问其他VLAN中服务器上的应用都很正常，如都能正常访问VLAN 3中的E-MAIL服务器。而且办公网和业务网中除了VLAN 12，其他VLAN中的用户，都能正常访问流媒体服务器，也就是只有VLAN 12中的用户访问不了。因为流媒体应用是单位业务中一项很重要的应用，若长时间不能用的话，可能会影响到公司业务正常运转，所以必须尽快排除故障。

2. 排查故障的步骤

(1)通过对故障信息的收集，我们确定了网络故障的大概示意图，如图1-15所

示。不能访问流媒体服务器的用户IP地址的网络号都是192.168.12.0/24。他们访问流媒体服务器的路径先是到Cisco3560，通过Cisco4507，最后到达服务器。

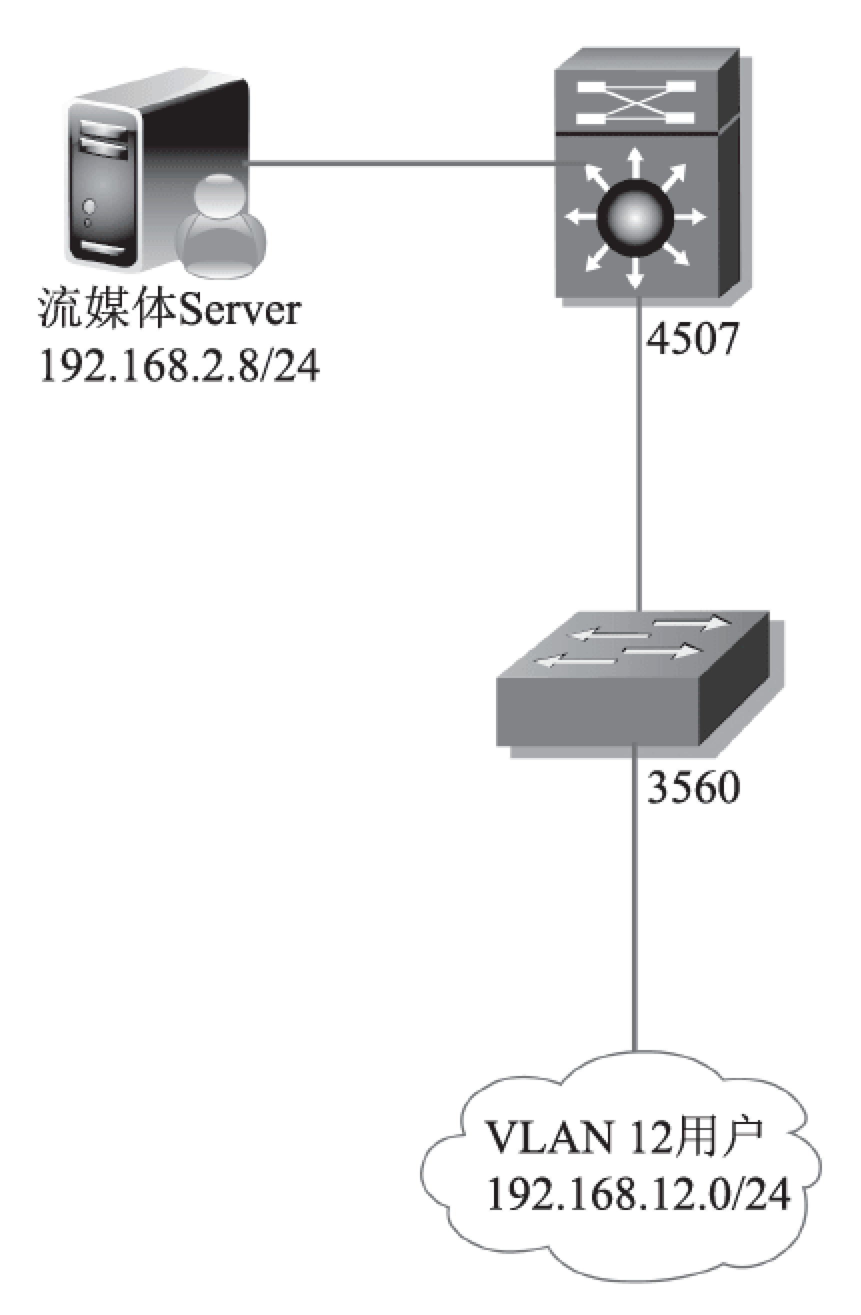


图1-15　存在故障的网络示意图

(2)我们到不能访问流媒体服务器的部门，查看了用户的PC，发现电脑上的IP地址、默认网关、DNS都是正确的。然后我们在用户电脑的“命令行”中执行“ping 192.168.2.8”命令，结果ping不通。然后又执行了ping VLAN 12网关地址的命令“ping 192.168.12.254”，发现能ping通。为了确定出具体的故障部位，又在“命令行”中执行了“tracert 192.168.2.8”命令，显示的结果如下所示：

```
C:\ >tracert 192.168.2.8
Tracing route to 192.168.2.8 over a maximum of 30 hops
  1    <1 ms    <1 ms    <1 ms  192.168.12.254
  2    *        *        *      Request timed out.
  3    *        *        *      Request timed out.
```

上面命令的显示结果还有27行省略了，因为数据包不能到达目的地，后面27项和第2、3项的内容一样。

从上面的结果可以看出，用户访问流媒体服务器时，数据包只能到达192.168.12.254，再往下路径就发生了故障，不能到达目的地。从前面的介绍知道Cisco3560上是没有IP地址配置的，它们都是作为二层交换机接入到网络中的，所有三层的地址都是在Cisco4507上配置的。也就是用户访问流媒体服务器的数据能到达4507，然后再往下就不知道哪出现了故障。可能是流媒体服务器故障，也可能是连接流媒体服务器和核心交换机4507之间的链路发生了故障。

(3)为了确定是服务器故障，还是服务器和4507之间链路的故障。我们把连接服务器的千兆网线接头拔下来，然后把接头接入到一台状态良好的PC上，PC上的IP地址、默认网关、DNS的配置和流媒体服务器上的配置完全一样。接着，再次在不能访问流媒体应用的用户电脑上执行了“ping 192.168.2.8”，结果一切正常，网络是通的。

(4)到现在就能确定，问题出现在流媒体服务器上。不过，现在还不能确定是服务器上流媒体的应用系统有问题，还是服务器上的网络设置方面有问题。接着我们查看了服务器上网络方面的设置，如图1-16所示，是在服务器“命令行”中执行“ipconfig /all”显示出的结果。

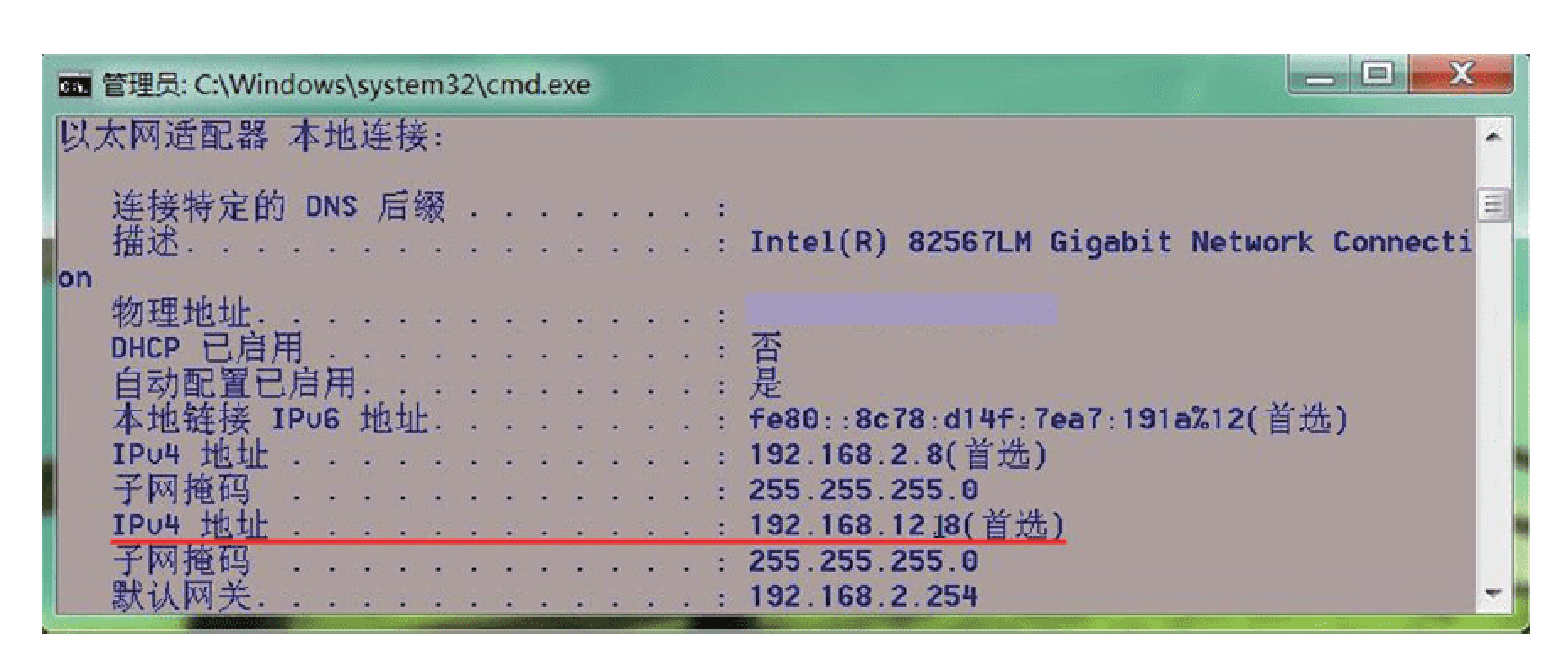


图1-16　流媒体服务器的IP地址配置

到这里已基本确定引起网络故障的原因，就是因为在流媒体服务器的网卡上配置了两个IP地址，其中192.168.12.18/24就是引起故障的错误配置。

(5)在流媒体服务器控制面板的“网络连接”中，找到和IP地址192.168.2.8对

应的“本地连接”，然后双击“本地连接”图标，在“属性”→“Internet协议(TCP/IP)属性”→“高级”，找到了添加错误IP地址192.168.12.18的地方，如图1-17所示。

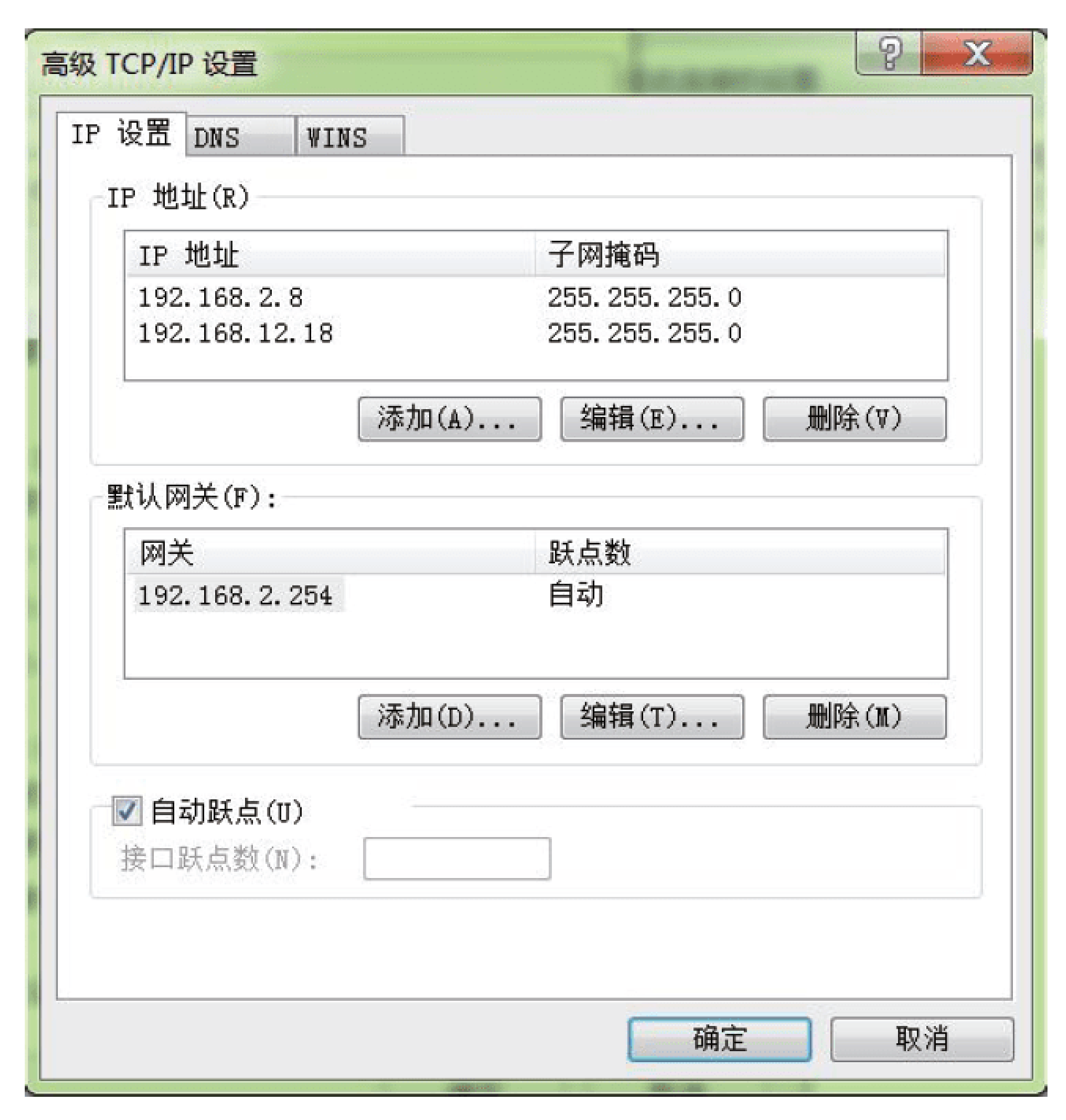


图1-17　添加/删除IP地址示意图

在图1-17中，选中IP地址192.168.12.18，然后单击“删除”按钮，就把网卡上错误的IP地址删除了。这时，VLAN 12中的用户也可以正常访问流媒体服务器中的应用了。

3. 总结

(1)如图1-18所示，是网络故障期间，在流媒体服务器的“命令行”中执行“route print”命令得到的结果。其中，红线标出的，就是上面在用户的电脑上执行“tracert 192.168.2.8”命令后，数据包不能从流媒体服务器返回到VLAN 12用户PC的原因所在。

```
管理员: C:\Windows\system32\cmd.exe
IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0    192.168.2.254      192.168.2.8    276
        127.0.0.0        255.0.0.0            在链路上         127.0.0.1    306
        127.0.0.1  255.255.255.255            在链路上         127.0.0.1    306
  127.255.255.255  255.255.255.255            在链路上         127.0.0.1    306
      192.168.2.0    255.255.255.0            在链路上       192.168.2.8    276
      192.168.2.8  255.255.255.255            在链路上       192.168.2.8    276
    192.168.2.255  255.255.255.255            在链路上       192.168.2.8    276
     192.168.12.0    255.255.255.0            在链路上       192.168.2.8    276
    192.168.12.18  255.255.255.255            在链路上       192.168.2.8    276
   192.168.12.255  255.255.255.255            在链路上       192.168.2.8    276
        224.0.0.0        240.0.0.0            在链路上         127.0.0.1    306
        224.0.0.0        240.0.0.0            在链路上       192.168.2.8    276
  255.255.255.255  255.255.255.255            在链路上         127.0.0.1    306
  255.255.255.255  255.255.255.255            在链路上       192.168.2.8    276
===========================================================================
永久路由:
  网络地址          网络掩码  网关地址  跃点数
          0.0.0.0          0.0.0.0    192.168.2.254     默认
===========================================================================
```

图1-18　流媒体服务器中的路由表

因为在VLAN 12中的用户PC上执行“tracert 192.168.2.8”的命令后，Tracert数据包中的目的IP地址是192.168.2.8，PC根据电脑中的默认网关地址192.168.12.254，先把数据包传输到Cisco3560，然后再到达Cisco4507。4507查看了Tracert数据包中的目的IP地址是192.168.2.8，知道它是要去往VLAN 2中的，然后4507把Tracert数据包传输到流媒体服务器。

当流媒体服务器收到Tracert数据包后，发现数据包的目的IP地址正是自己的IP地址，它把数据包收下后。然后根据Tracert命令的约定，它还要给VLAN 2中的用户PC返回一个Tracert数据包，这时返回的这个数据包的目的IP地址，对应的网络地址就是192.168.12.0/24，接着流媒体服务器就在自己的路由表查找到达目的网络192.168.12.0/24的路由，结果它就在自己的路由表中就找到了图1-18中红线标出的路由项目，在其中它找到网络192.168.12.0/24，是和自己的链路，也就是网卡直接相连的，因为路由项目中显示的“网关”对应项是“在链路上”。这种情况下流媒体服务器就不会把要返回的Tracert数据包路由到VLAN 2之外。结果VLAN 12中的用户也就不会收到返回的Tracert数据包。

(2)通常在计算机网卡、交换机和路由器的端口上都能配置两个或多个IP地址，在前两者上的主要作用是为了实现连接在同一局域网上不同网段之间的通信。一般由于一个网段中所包含的IP地址对于用户来说不够用，就可以采用配置多个IP地址的办法来扩大接入到局域网中用户的数量。而在路由器的端口上配置两个或多个IP地址主要是实现连在同一路由器端口的不同网段的通信，但这时要注意启用端口上的IP重定向功能，因为一般路由器不允许从同一端口进来的IP数

据包又发回到原端口中。启用了重定向功能，就允许在同一端口进入路由器的IP数据包由原端口再发送回去。但是在计算机网卡、交换机和路由器的端口上配置多个IP地址常常会给网络带来意想不到的故障，所以一般没有特殊需求，不要在同一端口上配置多个IP地址。

(3)这次公司流媒体服务器的故障也是因为在故障的前一天晚上，负责流媒体应用系统软件开发的厂商在公司调试软件，因为软件测试的需要，要在流媒体服务器的网卡上临时再配置一个IP地址，技术人员就随便配置了192.168.12.18这个地址。测试完成后，技术人员离开公司时忘了把这个IP地址删除掉，结果就导致了第二天早上的网络故障。

按照规定，对机房服务器上每一步重要的操作，都要记录在服务器日志登记本上。完成操作后，要逐项查看登记本，是否把服务器恢复到了初始的正常状态。但因为双方的技术人员都没有严格执行机房管理规定，从而造成了意外的疏漏。看来网络管理无小事，必须从点滴做起，从我做起。

1.5　运维实例：深刻理解HSRP

HSRP(Hot Standby Router Protocol)热备份路由器协议，即多台路由器组成一个“热备份组”，模拟成一个虚拟的路由器，虚拟路由器拥有虚拟的IP 地址和虚拟的MAC地址。在一个热备份组中，只有一台路由器作为活动路由器转发数据包，只有当活动路由器失效后，才会选择一台备份路由器作为活动路由器，但对于网络中的主机来说，虚拟路由器并没有发生任何改变，不会导致主机通信中断现象。

下面通过一则实例，通过介绍其配置和运行过程，将能更好地理解HSRP协议的作用。

1. 网络拓扑结构介绍

网络拓扑图如图1-19所示。两台核心交换机型号为Cisco Catalyst 4507R，每台4507R上使用两块引擎，Cisco Catalyst 4507R上两块引擎的名称分别为4507A-R1、4507A-R2，4507B上的分别为4507B-R1、4507B-R2。4507A和4507B通过

Trunk口连接，4507A和3750A，4507B和3750B之间也是通过Trunk口连接。4台交换机中都运行VTP协议，其中4507A中VTP运行模式是server模式，其他3台交换机中VTP运行的模式是client模式，并且在4507A中创建了VLAN 100和VLAN 200。

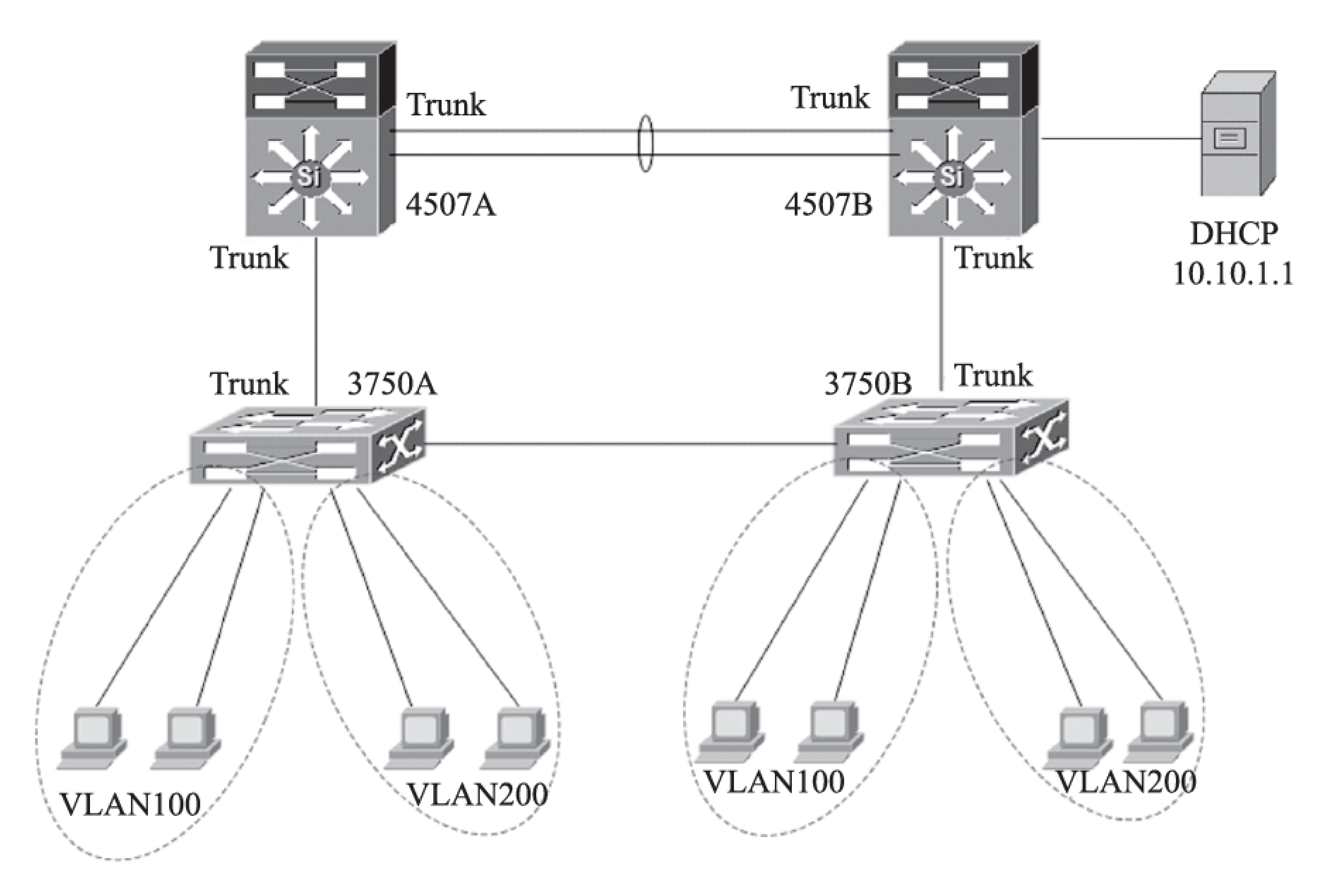


图1-19　络结构图

两台3750交换机上共接入了8台PC，VLAN 100和VLAN 200中各分配4台。8台电脑自动获取IP地址、默认网关、DNS服务器地址，这些地址都是通过DHCP服务器自动分配的。DHCP服务器的IP地址配置为10.10.1.1/24。网络的搭建也充分考虑了核心交换机的冗余性，若4507B故障，则3750B上的数据可先到达3750A，最后再到达核心交换机4507A。同理，若4507A故障，也不影响3750A上的数据到达核心交换机4507B。

2. DHCP服务器的配置

DHCP服务器的配置如图1-20和图1-21所示。需要说明的是，VLAN 100的默认网关要指向10.10.100.254，而不是10.10.100.253或10.10.100.252。同理，VLAN 200的默认网关也要指向10.10.200.254。

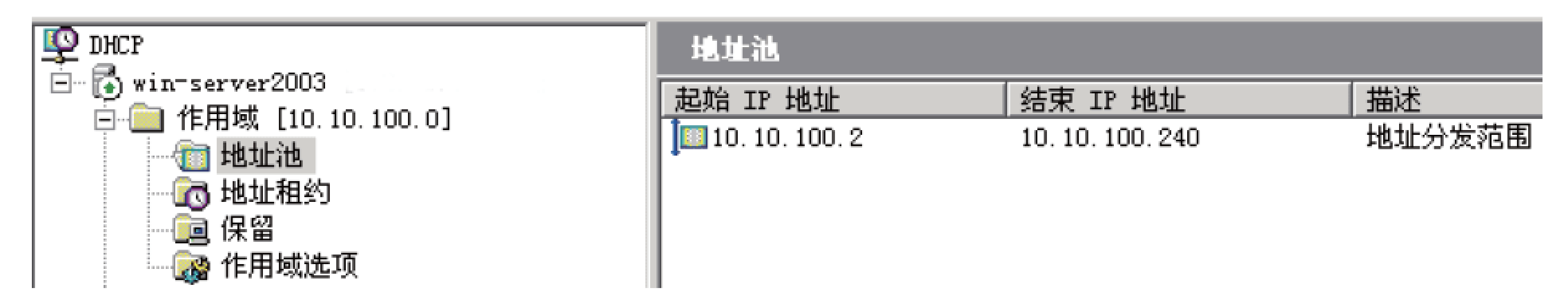


图1-20 VLAN 100的DHP配置



图1-21 VLAN 200的DHCP配置

3. HSRP配置的详细说明

4507A引擎1上的HSRP配置如下所示：

```
4507A-R1
interface VLAN100
 ip address 10.10.100.253  255.255.255.0
 ip helper-address 10.10.1.1
 standby 100 priority 150 preempt
 standby 100 ip 10.10.100.254
!
interface VLAN 200
 ip address 10.10.200.253  255.255.255.0
ip helper-address 10.10.1.1
 standby 200 priority 150 preempt
 standby 200 ip 10.10.200.254
```

其中命令“ip address 10.10.100.253 255.255.255.0”是给指定的VLAN配置IP地址。

命令“ ip helper-address 10.10.1.1”是确保两台3750交换机上的所有主机获取IP地址、默认网关和DNS服务器地址时，是从10.10.1.1的DHCP服务器上自动获取到的。

命令“standby 100 priority 150 preempt”中的“priority”是配置HSRP的优先级，100为组序号，它的取值范围为0～255，150为优先级的值，取值范围为0～255，数值越大优先级越高。

优先级将决定一台路由器在HSRP备份组中的状态，优先级最高的路由器将成为活动路由器，其他优先级低的路由器将成为备用路由器。当活动路由器失效后，备用路由器将替代它成为活动路由器。当活动和备用路由器都失效后，其他路由器将参与活动和备用路由器的选举工作。优先级都相同时，接口IP地址高的将成为活动路由器。

“preempt”是配置HSRP为抢占模式。如果需要高优先级的路由器能主动抢占成为活动路由器，则要配置此命令。配置preempt后，能够保证优先级高的路由器失效恢复后总能成为活动路由器。活动路由器失效后，优先级最高的备用路由器将处于活动状态，如果没有使用preempt技术，则当活动路由器恢复后，它只能处于备用状态，先前的备用路由器代替其角色处于活动状态。

命令“standby 100 ip 10.10.100.254”作用是启动HSRP，如果虚拟IP地址不指定，路由器就不会参与备份。虚拟IP应该是接口所在的网段内的地址，不能为接口上的IP地址。

4507A引擎2上HSRP的配置如下：

```
4507A-R2
interface VLAN100
 ip address 10.10.100.252  255.255.255.0
 ip helper-address 10.10.1.1
```

```
 standby 100 priority 140 preempt
 standby 100 ip 10.10.100.254
!
interface VLAN 200
 ip address 10.10.200.252  255.255.255.0
ip helper-address 10.10.1.1
 standby 200 priority 140 preempt
 standby 200 ip 10.10.200.254
```

由以上命令可知，当4507A引擎1和引擎2都在网络中运行时，引擎1是主状态，引擎2处于备用状态，因为引擎1的优先级150大于引擎2的优先级140。当然，若引擎1故障，引擎2就马上替代引擎1，并且不会引起网络的中断。

4507B引擎1和引擎2上HSRP的配置如下所示：

```
4507B-R1
interface VLAN100
 ip address 10.10.100.251  255.255.255.0
 ip helper-address 10.10.1.1
 standby 100 priority 130 preempt
 standby 100 ip 10.10.100.254
!
interface VLAN 200
 ip address 10.10.200.251  255.255.255.0
ip helper-address 10.10.1.1
```

```
 standby 200 priority 130 preempt
 standby 200 ip 10.10.200.254


4507B-R2
interface VLAN100
 ip address 10.10.100.250  255.255.255.0
 ip helper-address 10.10.1.1
 standby 100 priority 120 preempt
 standby 100 ip 10.10.100.254
!
interface VLAN 200
 ip address 10.10.200.250  255.255.255.0
 ip helper-address 10.10.1.1
 standby 200 priority 120 preempt
 standby 200 ip 10.10.200.254
```

从以上配置可以看到，若两个4507上的4块引擎都处于运行状态，则4507A上的引擎1处于活跃状态，因为引擎1的优先级在4块引擎中最高，其他3块引擎处于备用状态。若4507A的引擎1故障，则其他优先级高的引擎会马上由备用状态转换为活跃状态，从而保证了网络不会中断。

两台核心交换机4507A和4507B使用4块引擎，也极大提高了网络中核心交换机的稳定性和冗余能力。同一台4507上的某一块引擎故障，这台4507上的另一块引擎会马上被激活，并代替故障的引擎。若同一台的两块引擎板都故障，也不会影响核心交换机的路由功能，因为另一台4507上的引擎会马上被激活，担负起路由的任务。

4. 总结

HSRP技术应用在OSI参考模型的第三层，也就是在二层或者二层交换机上不存在HSRP技术的应用。

(1)HSRP技术保证了网络中路由器运行的高度可靠性。在HSRP路由体系中共包括3种路由器：一是活动路由器，负责转发，发送到虚拟路由器的数据。它通过基于UDP端口号为1985的广播，发送Hello消息，来通告它的活跃状态；二是备用路由器，监视HSRP组中的运行状态，并且在当前活跃路由器不可用时，迅速承担起负责数据转发的任务。备用路由器也发送Hello消息来通告组中其他路由器它备份路由器的角色：三是虚拟路由器，对最终的用户来说，它代表一台能持续工作的路由器设备。它有自己的MAC和IP地址。但实际上它是不转发数据包的，它的作用仅仅是代表一台可用的路由设备。

通过在配置了HSRP协议的路由器之间广播HSRP优先级，HSRP协议选出当前的活跃路由器。当在预先设定的一段时间内活跃路由器不能发送Hello消息时，优先级最高的备用路由器变为活跃路由器。为了减少网络的数据流量，在设置完活跃路由器和备用路由器之后，只有活跃路由器和备用路由器定时发送HSRP报文。

(2)在使用HSRP技术时，一些查看和调试的命令也很重要，如：“show standby brief”命令是显示路由器上一些HSRP简要的信息。另外还有很多调试命令，如“debug standby events detail”命令是显示HSRP事件；命令“debug standby error”是显示HSRP错误。

1.6　运维实例：网络设备热备部署的3种模式

在网络和数据中心的核心区域，网络和服务器的热备部署已是非常普遍的部署模式。下面就用3则实例介绍网络中网络设备常用的热备部署模式，以便大家在以后的工作中，能够根据自己的网络实际情况，选择正确的网络设备热备部署模式。

1. 二层交换机的热备份部署模式

这种热备份部署模式在网络中也是最常见、最简单的部署方式，一般在网络的分布层比较常见。为了实现交换机的冗余性，或者为了保障连接在交换机上的服务器的持续稳定运行，通常采用这种部署方式。因为服务器的运行，一般都要保证7×24小时的连续运转。所以，采用这种部署模式也比较合适。如图1-22所示，是二层交换机的热备份部署拓扑图，共包括两台Cisco2960交换机和两台服务器，结构比较清晰。

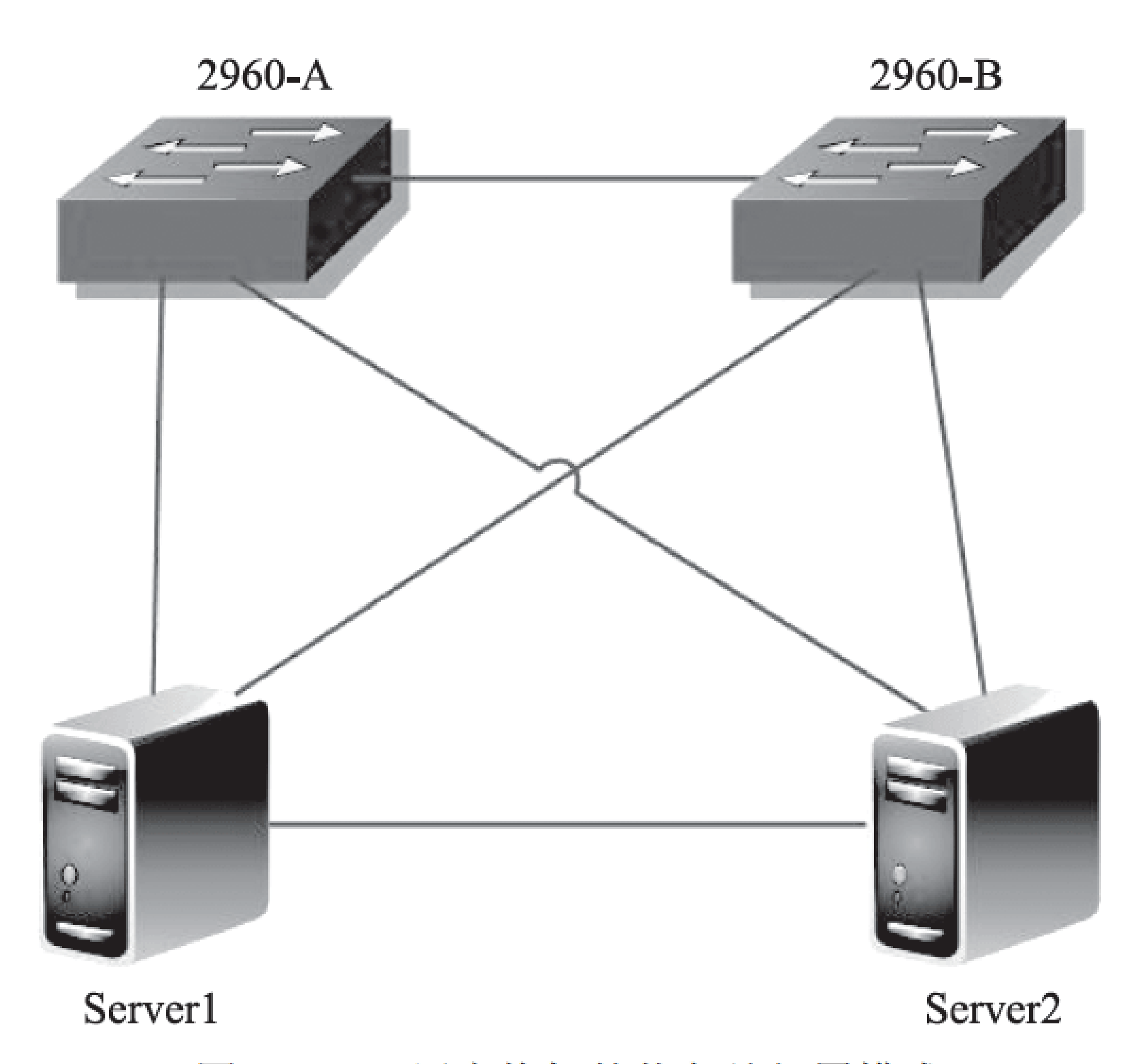


图1-22　二层交换机的热备份部署模式

设备间的连接情况如下所示：

```
Cisco2960A GigabitEthernet0/1 <-----> Server1 Eth0
Cisco2960A GigabitEthernet0/2 <-----> Server2 Eth0
Cisco2960B GigabitEthernet0/1 <-----> Server1 Eth1
Cisco2960B GigabitEthernet0/2 <-----> Server2 Eth1
Cisco2960A GigabitEthernet0/24 <-----> Cisco2960B GigabitEthernet0/24
Server1 Eth2 <-----> Server2 Eth2
```

Server1的IP地址为192.168.2.11，子网掩码为255.255.255.0，Server2的IP地址为192.168.2.12，子网掩码为255.255.255.0。两台服务器上的Eth0和Eth1两块网卡是绑定在一起的，例如Server1的Eth0和Eth1的两块网卡与外部进行数据通信时，两个网卡使用的IP地址都是192.168.2.11/24，若一块网卡故障的话，另一块网卡会继续保持与外界的通信，并不会影响服务器的正常运行。目前，有很多软件都能实现这种双网卡绑定的功能，例如RoseHA、NIC Express等。

Server1和Server2是主备模式运行，它们之间的网线连接相当于一条心跳线。两台服务器都安装有双机软件，双机软件时刻监控主备Server的各项参数，并通过心跳线传输控制信息。

双机软件监控的参数可以是服务器的网卡、数据库以及各种应用的运行情况等，若发现其中的任意一项参数不正常，双机软件都会通过心跳线传输控制信息，从而让备用服务器变为活动服务器，以接管原来主服务器的各项应用，而让原来的主服务器变为备服务器。在这种情况下，外界的用户根本感觉不到后台服务器的切换，也就不影响用户对各种应用的体验。

Cisco2960A的主要配置如下所示：

```
hostname Cisco2960A
!
interface GigabitEthernet0/1
 description LinkServer1Eth0
 switchport access VLAN 2
 switchport mode access
!
interface GigabitEthernet0/2
 description LinkServer2Eth0
 switchport access VLAN 2
```

```
 switchport mode access
!
interface GigabitEthernet0/24
 description Link2960B_0/24
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 2
 switchport mode trunk
!
interface VLAN 2
 ip address 192.168.2.1 255.255.255.0
 !
ip default-gateway 192.168.2.254
```

Cisco2960B上的主要配置如下所示：

```
hostname Cisco2960B
!
interface GigabitEthernet0/1
 description LinkServer1Eth1
 switchport access VLAN 2
 switchport mode access
!
interface GigabitEthernet0/2
 description LinkServer2Eth1
```

```
 switchport access VLAN 2
 switchport mode access
!
interface GigabitEthernet0/24
 description Link2960A_0/24
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 2
 switchport mode trunk
!
interface VLAN 2
 ip address 172.16.2.2 255.255.255.0
 !
ip default-gateway 172.16.2.254
```

两台交换机通过Trunk线连接，这样图1-22中的4台设备实际上都处于同一个VLAN，即VLAN 2中。两台交换机上VLAN 2的IP地址是作为管理地址使用的，这样用户在两台服务器上，也可以通过远程登录到交换机上，对交换机进行远程配置和管理。

这种配置模式可以保证两台交换机中的任意一台故障的话，也不会影响服务器上业务的正常运行。例如Cisco2960A故障的话，Server1可以通过它上面的Eth1网卡连接到Cisco2960B，再连到网络中。Server2也可以通过它上面的Eth1连接到Cisco2960B，再连到网络中。同样，若是Cisco2960B故障的话，也不会影响两台服务器的正常运转。这种模式的应用也就避免了交换机和服务器的单点故障。

2. 三层网络设备的热备份部署模式

上面的例子中，使用的网络设备是Cisco2960，属于二层设备。如果网络设备是三层设备，如三层交换机或路由器的话，要实现热备的功能，就需要

应用到具体的协议。若是Cisco的设备，可以使用HSRP、VRRP和GLBP协议。HSRP(Hot Standby Router Protocol，热备份路由器协议)和GLBP(Gateway Load Balancing Protocol，网关负载均衡协议)是思科专有协议，只能在思科设备上使用。而VRRP(Virtual Router Redundancy Protocol，虚拟路由冗余协议)是公有协议，既可以在思科设备上使用，也可以在H3C设备上使用。

下面就以三层交换机Cisco3750为例，介绍HSRP协议在网络设备热备份功能上的应用。如图1-23所示，网络结构图和“1”中的网络结构一样，只是网络设备换成了Cisco3750。

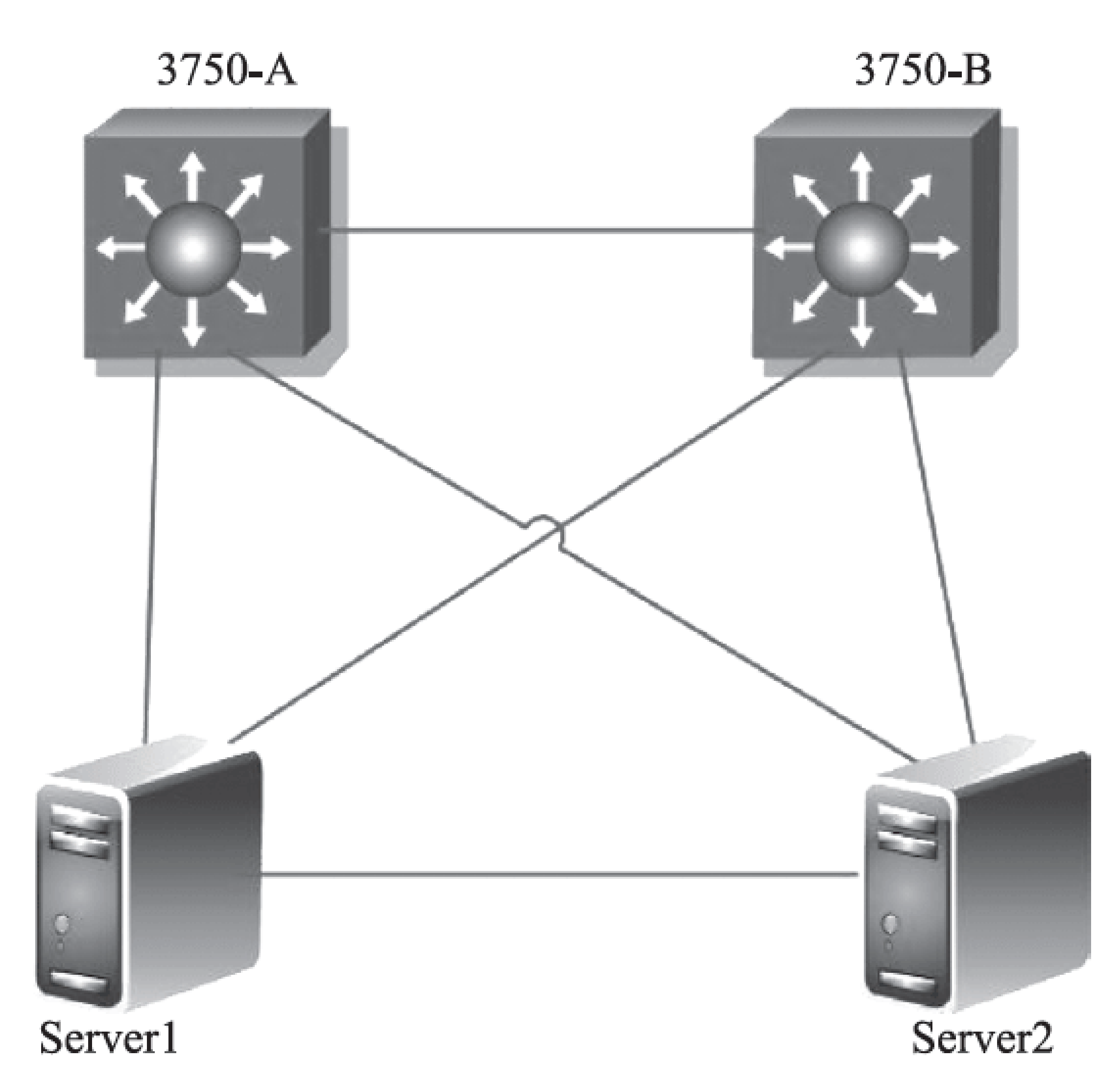


图1-23　三层网络设备的热备份部署模式

设备间的连接情况如下所示：

```
    Cisco3750A GigabitEthernet1/0/1 <-----> Server1 Eth0
    Cisco3750A GigabitEthernet1/0/2 <-----> Server2 Eth0
    Cisco3750B GigabitEthernet1/0/1 <-----> Server1 Eth1
    Cisco3750B GigabitEthernet1/0/2 <-----> Server2 Eth1
    Cisco3750A GigabitEthernet1/0/25 <----> Cisco3750B GigabitEthernet1/0/25
    Server1 Eth2 <-----> Server2 Eth2
```

在上面的连接中，Cisco3750A和Cisco3750B之间通过G1/0/25连接，使用的是光纤连接，而其他连接都使用的是双绞线。

在Cisco3750A上的主要配置如下所示：

```
hostname Cisco3750A
!
interface GigabitEthernet1/0/1
 description LinkServer1Eth0
 switchport access VLAN 2
 switchport mode access
!
interface GigabitEthernet1/0/2
 description LinkServer1Eth1
 switchport access VLAN 2
 switchport mode access
!
interface GigabitEthernet1/0/25
 description Link3750B_1/0/25
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 2
 switchport mode trunk
!
interface VLAN 2
 ip address 192.168.2.252 255.255.255.0
```

```
standby 2 ip 192.168.2.254
standby 2 priority 120
standby 2 preempt
```

其中命令“ip address 192.168.2.252 255.255.255.0”是给指定的VLAN配置IP地址。

命令“standby 2 priority 120”中的“priority”是配置HSRP的优先级，2为组序号，它的取值范围为0～255，120为优先级的值，取值范围为0～255，数值越大优先级越高。

优先级将决定一台路由器在HSRP备份组中的状态，优先级最高的路由器将成为活动路由器，其他优先级低的路由器将成为备用路由器。当活动路由器失效后，备用路由器将替代它成为活动路由器。当活动和备用路由器都失效后，其他路由器将参与活动和备用路由器的选举工作。优先级都相同时，接口IP地址高的将成为活动路由器。

“preempt”是配置HSRP为抢占模式。如果需要高优先级的路由器能主动抢占成为活动路由器，则要配置此命令。配置preempt后，能够保证优先级高的路由器失效恢复后总能成为活动路由器。活动路由器失效后，优先级最高的备用路由器将处于活动状态，如果没有使用preempt技术，则当活动路由器恢复后，它只能处于备用状态，先前的备用路由器代替其角色处于活动状态。

命令“standby 2 ip 192.168.2.254”作用是启动HSRP，如果虚拟IP地址不指定，路由器就不会参与备份。虚拟IP应该是接口所在的网段内的地址，不能配置为接口上的IP地址。

在Cisco3750B上的主要配置如下所示：

```
hostname Cisco3750B
!
interface GigabitEthernet1/0/1
```

```
 description LinkServer1Eth1
 switchport access VLAN 2
 switchport mode access
!
interface GigabitEthernet1/0/2
 description LinkServer2Eth1
 switchport access VLAN 2
 switchport mode access
!
interface GigabitEthernet1/0/25
 description Link3750A_1/0/25
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 2
 switchport mode trunk
!
interface VLAN 2
 ip address 192.168.2.253 255.255.255.0
 standby 2 ip 192.168.2.254
 standby 2 priority 120
 standby 2 preempt
```

另外，可以使用其他一些命令，查看HSRP的运行状态，如“debug standby events detail”命令是显示HSRP事件；命令“debug standby error”是显示HSRP错误。另外，还有命令“show standby brief”是显示路由器上一些HSRP简要的信息，如下所示是在Cisco3750A上执行此命令的显示结果：

```
Cisco3750A#show standby brief
                P indicates configured to preempt.
                |
Interface   Grp   Prio   P State    Active    Standby
Virtual IP
Vl2          2     120    P Active   local    172.16.81.252
172.16.81.254
```

这种部署模式中，服务器上的配置，及网线连接情况和“1”中的一样，也是双机热备部署模式。需要注意的是在两台服务器上配置IP地址时，默认网关的地址一定要写成192.168.2.254，不能写成192.168.2.252或192.168.2.253。因为Cisco3750中的VLAN 2和外部进行数据通信时，使用的就是192.168.2.254这个IP地址，而不是其他两个。

这种模式中，两台交换机同样可以起到热备的功能，任意一台交换机故障并不会影响到另外一台交换机和两台服务器的正常运行。也就解决了网络设备的单点故障。这种部署模式一般应用在网络的核心层，在高性能的三层交换机或路由器上进行部署，担负整个网络核心数据的路由、交换功能。

3. 网络设备热备份功能的混合部署模式

目前，在大部分的网络中，为了不影响用户对各种业务应用的连续不间断使用，在网络的核心层和分布层网络设备上，都使用了设备的热备份功能。下面的例子其实就是上面“1”和“2”两种部署模式的混合使用，如图1-24所示。只是在分布层使用的交换机为Cisco3750，而不是Cisco2960。因为在性能上3750还是比2960优越很多。只不过没有使用Cisco3750上的三层路由功能，而只使用了它的二层交换功能。

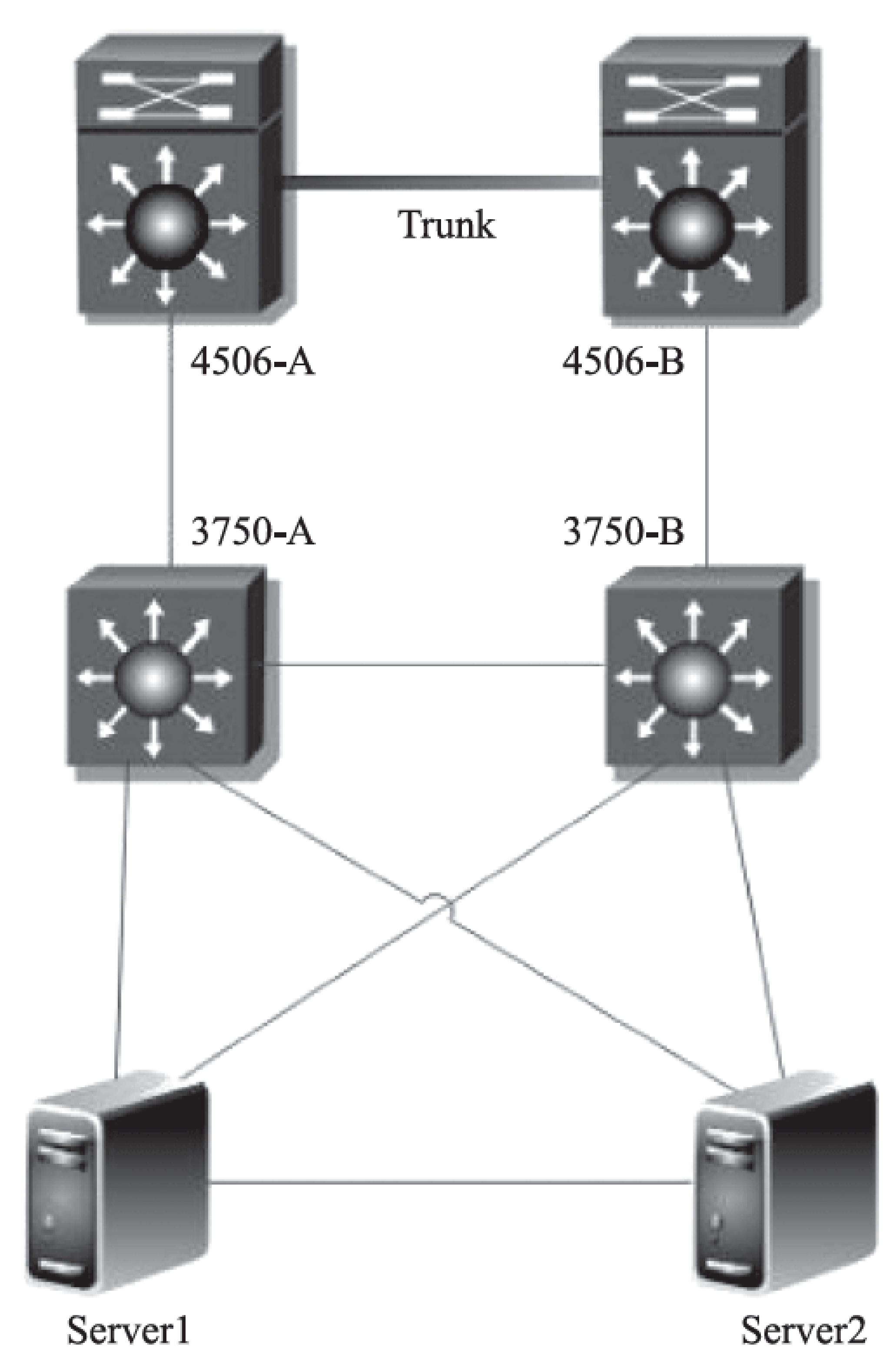


图1-24　网络设备热备份功能的混合部署模式

图1-24部署模式设备间的连接情况如下所示：

```
  Cisco4506A GigabitEthernet1/1 <----> Cisco4506B GigabitEthernet1/1
  Cisco4506A GigabitEthernet2/1 <----> Cisco3750A GigabitEthernet1/0/28
  Cisco4506B GigabitEthernet2/1 <----> Cisco3750B GigabitEthernet1/0/28
  Cisco3750A GigabitEthernet1/0/1 <-----> Server1 Eth0
  Cisco3750A GigabitEthernet1/0/2 <-----> Server2 Eth0
  Cisco3750B GigabitEthernet1/0/1 <-----> Server1 Eth1
  Cisco3750B GigabitEthernet1/0/2 <-----> Server2 Eth1
```

```
    Cisco3750A GigabitEthernet1/0/25 <----> Cisco3750B
GigabitEthernet1/0/25
    Server1 Eth2 <-----> Server2 Eth2
```

在上面的连接中，Cisco4506A和Cisco4506B之间的连接，Cisco4506和Cisco3750之间的连接及Cisco3750A和Cisco3750B之间的连接都是通过光纤连接的。而其他的连接使用的都是双绞线的连接。

在Cisco4506A和Cisco4506B上的主要配置和在“2”中Cisco3750上的配置基本一致，因为它们都是属于三层设备上的配置。

在Cisco4506A上的主要配置如下所示：

```
hostname Cisco4506A
!
interface GigabitEthernet1/1
 description Link4506B_1/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 2
 switchport mode trunk
!
interface GigabitEthernet2/1
 description Link3750A
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 2
 switchport mode trunk
!
```

```
interface VLAN 2
 ip address 192.168.2.252  255.255.255.0
standby 2 ip 192.168.2.254
 standby 2 priority 120
standby 2 preempt
```

在Cisco4506B上的主要配置如下所示：

```
hostname Cisco4506B
!
interface GigabitEthernet1/1
 description Link4506A_1/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 2
 switchport mode trunk
!
interface GigabitEthernet2/1
 description Link3750B
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 2
 switchport mode trunk
!
interface VLAN 2
ip address 192.168.2.253  255.255.255.0
```

```
standby 2 ip 192.168.2.254
 standby 2 priority 120
standby 2 preempt
```

在Cisco3750A和Cisco3750B上的主要配置和在上面“1”中的Cisco2960上的配置基本一致，因为它们都属于二层设备上的配置。

在Cisco3750A上的主要配置如下所示：

```
hostname Cisco3750A
!
interface GigabitEthernet1/0/1
 description LinkServer1Eth0
 switchport access VLAN 2
 switchport mode access
!
interface GigabitEthernet1/0/2
 description LinkServer1Eth1
 switchport access VLAN 2
 switchport mode access
!
interface GigabitEthernet1/0/25
 description Link3750B_1/0/25
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 2
```

```
 switchport mode trunk
!
interface GigabitEthernet1/0/28
 description Link4506A
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 2
 switchport mode trunk
!
interface VLAN 2
 ip address 192.168.2.1 255.255.255.0
ip default-gateway 192.168.2.254
```

在Cisco3750B上的主要配置如下所示：

```
hostname Cisco3750B
!
interface GigabitEthernet1/0/1
 description LinkServer1Eth1
 switchport access VLAN 2
 switchport mode access
!
interface GigabitEthernet1/0/2
 description LinkServer2Eth1
 switchport access VLAN 2
```

```
 switchport mode access
!
interface GigabitEthernet1/0/25
 description Link3750A_1/0/25
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 2
 switchport mode trunk
!
interface GigabitEthernet1/0/28
 description Link4506B
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 2
 switchport mode trunk
!
interface VLAN 2
 ip address 192.168.2.2 255.255.255.0
ip default-gateway 192.168.2.254
```

图1-24所示的部署模式，也是目前一些大、中型企业中常用的一种部署模式。一般核心层的网络设备不会太多，也就2～4台，但分布层中的设备，如图1-24中的Cisco3750就会部署很多台。可以根据单位部门的不同或不同的楼宇部署在不同的位置。在分布层的设备上一般还会连接有很多的接入层交换机，这些设备一般都不会使用热备份功能的部署模式。因为它们都是通过机房中的配线架直接就连接到了用户的电脑上了，若是有一台接入层的交换机故障了，它只是影响了很小的一部分用户。所以，网络中对接入层交换机的可靠性要求并不是很高，也就没有必要使用热备份的部署模式。

4. 总结

(1)HRSP主要用在源主机无法动态学习到网关IP地址的情况下，防止默认路由失败。它类似于服务器的HA群集，两台或更多的路由器以同样的方式配置成Cluster，创建出单个的虚拟路由器，然后客户端将网关指向该虚拟路由器，最后由HSRP决定哪个路由器扮演真正的默认网关。HRSP组里的每个成员路由器仍然是标准的路由器，客户端仍然可以将成员路由器配置成其默认网关。HRSP选择优先级最高的路由器为活动路由器。如果优先级相同，则IP地址高的成为活动路由器。在HRSP组中，只允许同时存在一个活动路由器，其他路由器都处于备用状态，备用路由器不转发数据包。如果备用路由器持续不断地收到活动路由器发来的Hello包，则其会一直处于备用状态。一旦备用路由器在规定的时间内没有收到Hello包，则认为活动路由器失效，优先级最高的备用路由器就接替活动路由器的角色，开始转发数据包。

VRRP是不同设备厂家之间共同遵循的标准。它负责从路由器组中选择一个作为Master，然后客户端使用虚拟路由器地址作为其默认网关。一个两成员的HSRP组必须使用三个地址，每个路由器一个实IP地址，HSRP组一个虚拟IP地址。而一个两成员的VRRP组只需要使用两个IP地址。Master设备的Interface IP即为VRRP组的虚拟IP地址。若Master设备故障后，备用的设备将接管该IP。不过VRRP也可以像HSRP一样使用两个实IP地址和一个虚IP地址。

GLBP不仅提供冗余网关，还在各网关之间提供负载均衡。而HRSP、VRRP都是选定一个活动路由器，备用路由器则处于闲置状态。和HRSP不同的是，GLBP可以绑定多个MAC地址到虚拟IP，从而允许客户端选择不同的路由器作为其默认网关，而网关地址仍使用相同的虚拟IP，从而实现一定的冗余功能。GLBP选举活动网关时，优先级最高的路由器成为活动路由器，其他非活动的则提供冗余功能。若某路由器被推举为活动路由器后，它就分配虚拟的MAC地址给其他GLBP组成员。所有的GLBP组中的路由器都转发数据包，但是各路由器只负责转发与自己的虚拟MAC地址相关的数据包。

(2)以上三种网络设备热备的部署模式主要是根据网络的规模和具体的实际应用情况进行选择部署。模式“1”和“2”从网络的拓扑上看没什么区别，但在模式1中所有数据都是在一个网段中进行传输的，也就是以广播的方式发送和传输数据。而在模式2中涉及到了不同网段之间数据的路由，它能把一个大的广播

域分割成多个更小的广播域，从而提高链路带宽的利用率。所以说模式1和模式2在运行本质上是不一样的。而部署模式3是模式1和2的综合，适用于更大型的网络。

1.7 运维实例：DHCP IP地址池扩充简单方案

网络的结构图如图1-25所示，核心交换机为Cisco4503，办公楼二层、三层汇聚层交换机为Cisco3750，其中在两台3750的下面还有接入层交换机，为了图示简洁没有画出。在4503和两台3750上都启用了思科VTP功能，其中4503的VTP运行模式是Server，两台3750的VTP运行模式为Client。两台3750和4503都是Trunk连接。二层、三层用户的客户端IP地址都是通过DHCP服务器自动分配的，二层所有的用户都在VLAN 2，三层的用户在VLAN 3，如图1-26所示。

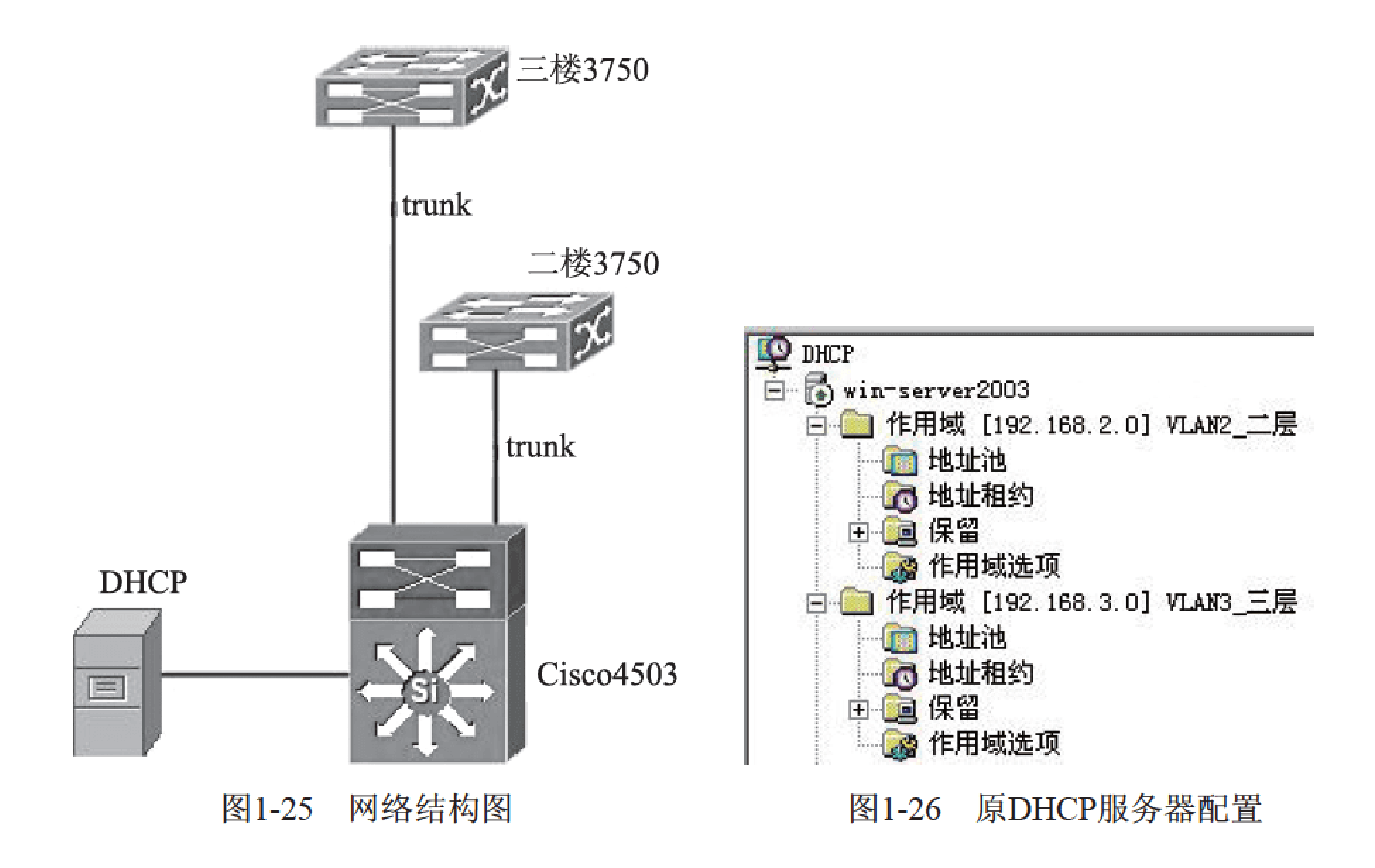


图1-25 网络结构图 图1-26 原DHCP服务器配置

由于最近二层、三层的部门新聘用了很多人员，而DHCP中二层VLAN 2能分配的最大IP地址数为252个，即192.168.2.2～192.168.2.253，而二层目前所有的用户数已超过252个。同样对于三层VLAN 3也存在这样的问题。在这种情况下，我们就想到了新增VLAN 12和VLAN 13两个网段，作为2、3网段的扩充，2和12网段等价，3和13网段等价。

因为4503的VTP运行模式是Server，所以只需在4503上创建VLAN 12和VLAN 13，两台3750上会自动创建VLAN 12和VLAN 13的。同时在4503上用(config)#interface VLAN命令创建SVI接口，并配置IP地址，即VLAN 12和VLAN 13的网关地址，如图1-27所示。最后，在DHCP服务器上创建VLAN 12和VLAN 13网段，如图1-28所示。这样就顺利实现了DHCP服务器IP地址池的扩容，从能容纳252个使用IP地址的用户数，扩充到252×2为504个。




```
Cisco4503(config)#interface vlan12
Cisco4503(config-if)#ip address 192.168.12.254 255.255.255.0
Cisco4503(config-if)#no shutdown
Cisco4503(config-if)#interface vlan13
Cisco4503(config-if)#ip address 192.168.13.254 255.255.255.0
Cisco4503(config-if)#no shutdown
```

图1-27　Cisco4503的配置　　　　图1-28　目前DHCP服务器配置

这样办公楼二层、三层新增加的用户，就可以分别接入到VLAN 12和VLAN 13中，这样就解决了2、3网段IP地址不够用的问题。

1.8　运维实例：明明白白NAT

目前，ICANN已把 IPv4地址分配完毕。按理说，一些组织多少应该有些紧张，因为没有了IP地址，怎么保证一些网络设备互联到Internet？这是因为目前许多单位普遍使用了NAT(Network Address Translation，网络地址转换)技术。下面就通过一则现实中运行的实例和一些截图让大家完全明白NAT运行的机制和原理。

1. 网络结构图说明

网络拓扑图如图1-29所示，分公司的PC(10.10.10.2/24)通过Internet访问总部的Server(192.168.10.2/24)。其中在分公司的Cisco3750上应用了PAT规则，也就是“端口NAT”。在公司总部的防火墙B上应用了Static NAT，并且防火墙B上的互

联网端口的IP地址配置为114.23.72.19/24。分公司Cisco3750上的互联网端口的IP地址配置为114.23.72.219/24。在分公司的PC电脑上和总部的Server上都运行了“360流量监控”软件，通过软件中的“网络连接”面板，能够清楚的看出NAT运行的机理。

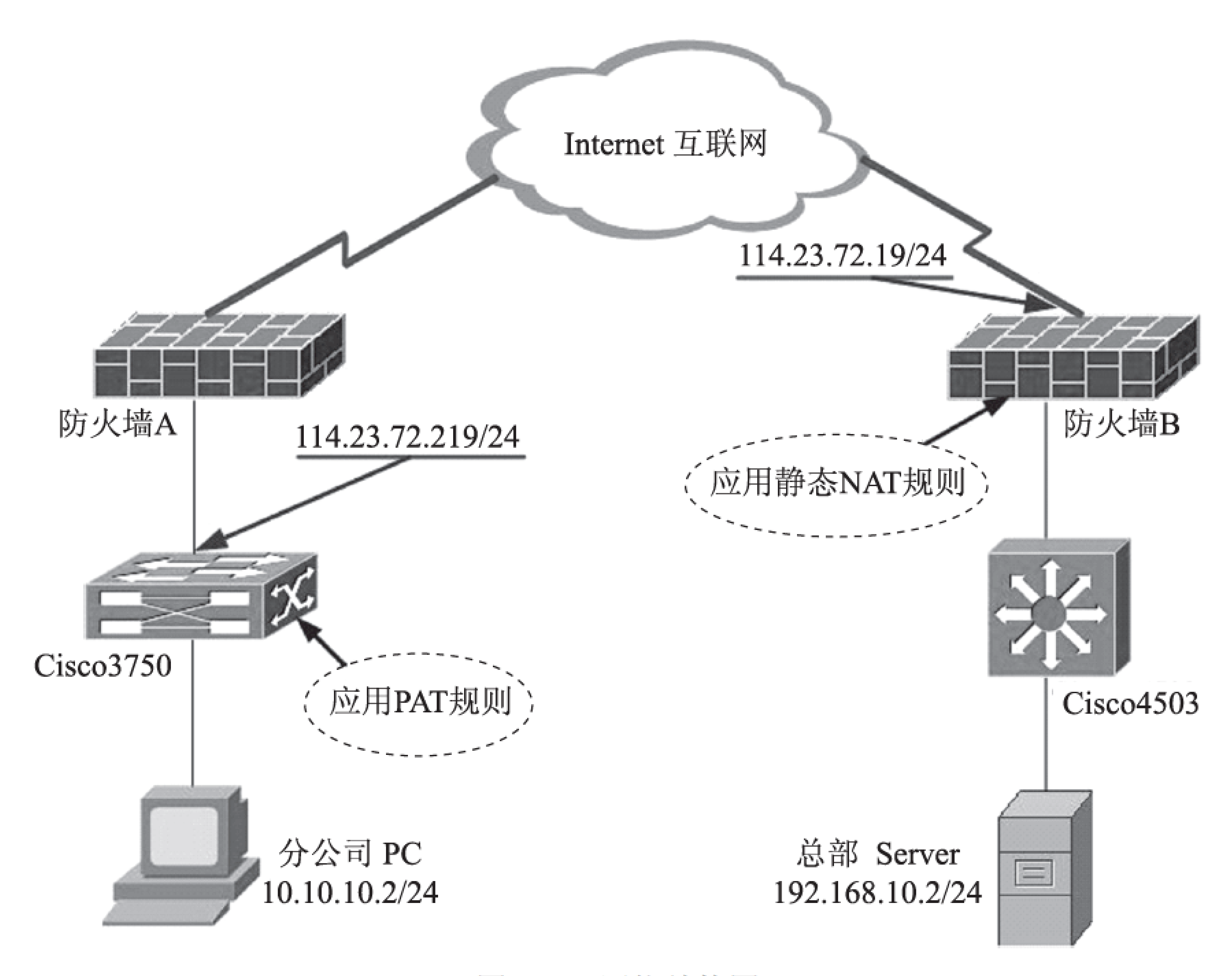


图1-29 网络结构图

2. 交换机和防火墙上NAT的配置

(1)总部防火墙B上应用的是Static NAT规则，通过防火墙的Web控制页面就可操作完成，即在114.23.72.19/24和192.168.10.2/24之间做一静态转换，并且这两个IP地址之间的服务端口也都是一一对应。

(2)Cisco3750上的配置文件如下所示：

```
ip nat pool corporation 114.23.72.219 114.23.72.219 netmask 255.255.255.0
\\定义内部全局地址池
ip nat inside source list 10 pool corporation overload
```

```
\\建立映射关系
    !
    interface GigabitEthernet1/0/1      \\定义外网接口
    no switchport
    ip address 114.23.72.219 255.255.255.0
    ip nat outside
    !
    interface GigabitEthernet1/0/10      \\定义内网接口
    ip nat inside
    !
    access-list 10 permit 10.10.10.0 0.0.0.255      \\定义内部本地地址范围
```

3. 实时监控查看NAT运行过程

“360流量监控”软件可以详细地显示本机服务和远程主机服务的连接情况。因为在大部分的电脑中，TCP 139端口都是默认打开的，这样只需在分公司PC的“命令行”中执行“telnet 114.23.72.19 139”命令，就可在分公司PC与总部Server之间建立一个TCP连接，这是因为Telnet应用是通过TCP建立连接的。建立连接后，就可通过“360流量监控”中的“网络连接”面板查看它们的连接情况。如图1-30所示，是在PC上“360流量监控”的截图。从图上可以看出，PC上启动了一个“Telnet.exe”的进程，进程使用的是TCP协议，在本地的7420端口和总部Server服务器的139端口建立了连接。



图1-30　分公司PC上360实时截图

图1-31所示是在Server上的“360流量监控”的截图。从图上可以看出，在总部Server上启动了一个“System”的系统进程，并且在本地的139端口和目标IP的52617端口之间建了TCP连接。



图1-31　总部Server上360实时截图

通过这两幅截图就能明白现实中NAT运行的原理。图中并没有显示出在10.10.10.2和192.168.10.2之间直接建立了连接，就是因为在Cisco3750和防火墙B上应用了NAT规则。

4. 总结

(1)NAT规则有3种类型：静态NAT(Static NAT)、动态NAT(Dynamic NAT)和端口NAT(PAT)，也称动态复用NAT。其实动态NAT就是静态NAT的一种特例。本实例中就应用了3种NAT规则中的两种，静态NAT和PAT。

静态NAT：将内部网络的私有IP地址转换为公有IP地址，IP地址对是一对一的，也是一直不变的。实例中总部的IP地址114.23.72.19和192.168.10.2之间就是这种一对一的转换。也就是某个私有IP地址只转换为某个公有IP地址。借助于静态NAT，可以实现外部网络对内部网络中某些特定服务器的访问。

动态NAT：将内部网络的私有IP地址转换为公用IP地址时，IP地址是不确定，随机的。所有被授权访问Internet的私有IP地址可随机转换为任何指定合法的IP地址。也就是说，只要指定哪些内部地址可以进行转换以及用哪些合法地址作为外部地址时，就可以进行动态NAT转换。动态NAT可以使用多个合法外部地址集。当ISP提供的合法IP地址略少于网络内部的计算机数量时，可以采用动态转换的方式。

PAT：改变外出数据包的源端口并进行端口转换，采用端口多路复用方式。内部网络的所有主机均可共享一个合法外部IP地址实现对Internet的访问，可以最大限度地节约IP地址资源。同时，也可以隐藏网络内部的所有主机，有效避免来自Internet的攻击。因此，目前网络中应用最多的就是PAT规则。

(2)NAT也能有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算

机。但NAT最主要的作用，是在一定程度上减缓了IPv4地址耗尽的进度，但它也只是减缓，并不能阻止。目前，再有组织申请IP地址，就只能是IPv6地址了。因为IPv6地址数量庞大，按保守方法估算，IPv6实际可分配的地址，在整个地球每平方米面积上可分配1000多个地址，号称能让“每颗沙子都拥有一个IP地址”。既然IPv6有这么多的地址，能保证每一个Internet上的终端使用的都是全球唯一IP地址，所以当IPv6地址在全球普及的时候，也是NAT技术消亡的时候。

第2章 网络二层协议

在计算机网络二层的各类技术和协议中，最常用到的就是VLAN和Trunk，MAC地址也是经常用到的。MAC(Media Access Control)，又称媒体访问控制，用来定义网络设备的位置。在OSI模型中，第二层数据链路层负责 MAC地址，其实工作在数据链路层的交换机，就是维护着计算机的MAC地址和自身端口的数据库，交换机根据收到的数据帧中的目的MAC地址字段来转发数据帧。因此一个主机会有一个MAC地址，MAC地址是网卡决定的，它实际上就是适配器地址，是由网卡生产厂家烧入网卡的EPROM闪存中，它存储的是传输数据时真正赖以标识发出数据的电脑和接收数据的主机的地址，而且是不可更改的。形象地说，MAC地址就如同我们身份证上的身份证号码，具有全球唯一性。

VLAN(Virtual Local Area Network)，又称虚拟局域网，是指在交换局域网的基础上，采用网络管理软件构建的可跨越不同网段、不同网络的端到端的逻辑网络。一个VLAN组成一个逻辑子网，即一个逻辑广播域，它可以覆盖多个网络设备，允许处于不同地理位置的网络用户加入到一个逻辑子网中。Trunk技术用在交换机之间互连，使不同VLAN通过共享链路与其他交换机中的相同VLAN通信。交换机之间互连的端口就称为Trunk端口。

2.1　网络二层协议概述

2.1.1　MAC地址

MAC地址，采用十六进制数表示，共6个字节48位。其中，前3个字节是由IEEE的注册管理机构负责分配给不同厂家的代码，也就是高位24位，称为组织上唯一的标识符。后三个字节，也就是低位24位，由各厂家自行指派给生产的适配器接口，称为扩展标识符，一个地址块可以生成224个不同的地址。

在网络中，最常用的两个地址就是IP地址和MAC地址，IP地址专注于网络层，将数据包从一个网络转发到另外一个网络，而MAC地址专注于数据链路

层，将一个数据帧从一个节点传送到相同链路的另一个节点。网络层设备，如路由器根据IP地址来进行操作。数据链路层设备，如交换机根据MAC地址来进行操作。在一个稳定的网络中，IP地址和MAC地址是成对出现的。如果一台计算机要和网络中另一外计算机通信，那么要配置这两台计算机的IP地址，配置的IP地址就和MAC地址形成了一种对应关系。在数据通信时，IP地址负责表示计算机的网络层地址。IP和MAC地址这种映射关系由ARP地址解析协议完成的。

IP地址和MAC地址相同点是它们都是唯一的，不同点主要有三点：一是对于网络上的某一设备，如一台计算机或一台路由器，其IP地址是基于网络拓扑设计出的。同一台设备或计算机上，改动IP地址是很容易的，而MAC则是生产厂商烧录好的，一般不能改动。二是IP地址和MAC地址的长度也是不同的，IP地址为32位，MAC地址为48位。三是IP地址应用于OSI第三层，即网络层，IP地址的分配是基于网络拓扑，而MAC地址应用在OSI第二层，即数据链路层，MAC地址的分配是基于制造商。

2.1.2　VLAN技术

VLAN工作在OSI参考模型的第二层和第三层，VLAN之间的通信是通过第三层的路由器来完成的。因此VLAN间的通信也需要路由器提供中继服务，这被称作“VLAN间路由”。VLAN是广播域(指的是目标MAC地址全部为1的广播帧，所能传递到的范围，亦即能够直接通信的范围)，广播域之间来往的数据包都是由路由器中继的。本来二层交换机只能构建单一的广播域，不过使用VLAN功能后，它能够将网络分割成多个广播域。

与传统的局域网技术相比较，VLAN技术更加灵活。使用VLAN技术网络设备的移动、添加和修改的管理开销减少，也可以控制广播活动，还可以提高网络的安全性。在计算机网络中，一个二层网络可以被划分为多个不同的广播域，一个广播域对应了一个特定的用户组，默认情况下这些不同的广播域是相互隔离的。

2.1.3　Trunk技术

Trunk能够实现不同交换机中同一VLAN间数据的通信，但是Trunk技术不能

实现不同VLAN间通信，需要通过使用三层设备，用路由或三层交换机来实现。

两台交换机上分别创建了多个VLAN，在两台交换机上相同的VLAN，例如VLAN 8要通信，需要将交换机A上属于VLAN 8的一个端口与交换机B上属于VLAN 8的一个端口互连，如果这两台交换机其他相同VLAN间需要通信，那么交换机之间需要更多的互连线，端口利用率就太低了。若交换机使用trunk技术，事情就简单多了，只需要两台交换机之间有一条互连线，将互连线的两个端口设置为trunk模式，这样就可以使交换机上不同VLAN共享这条线路。

交换机的端口一般有两种模式：access和trunk。连接终端，如PC使用access模式，设备间级联若要传输多个VLAN中的数据，则用trunk模式。把access端口加入到某个VLAN，那么这个端口就只将这个VLAN的数据转发给PC，PC发送的数据通过这个端口后会打上这个VLAN的ID，转发到相同VLAN。

2.1.4 VTP协议

VTP(VLAN Trunking Protocol，VLAN中继协议)，也被称为虚拟局域网干道协议。不过有一点要记住它是思科私有协议，在华为、锐捷等交换机上是不支持此协议的。有时我们需要在整个园区网或者企业网中的一组交换机中保持VLAN数据库的同步，以保证所有交换机都能从数据帧中读取相关的VLAN信息进行正确的数据转发，然而对于大型网络来说，可能有成百上千台交换机，而一台交换机上都可能存在几十乃至数百个VLAN，如果仅凭网络工程师手工配置的话是一个非常大的工作量，并且也不利于日后维护——每一次添加修改或删除VLAN都需要在所有的交换机上部署。这种情况下，使用VTP是最好的选择，把一台交换机配置成VTP Server，其余的交换机配置成VTP Client，这样模式是Client的交换机就可以自动学习到Server上的VLAN信息，大大减轻了网络运维人员的工作量。

VTP是一个位于OSI参考模型第二层的通信协议，主要用于管理在同一个域的网络范围内VLAN的建立、删除和重命名。在一台VTP Server上配置一个新的VLAN时，该VLAN的配置信息将自动传播到本域内的其他所有交换机。这些交换机会自动地接收这些配置信息，使其VLAN的配置与VTP Server保持一致，从而减少在多台设备上配置同一个VLAN信息的工作量，而且保持了VLAN配置的

统一性。VTP在系统级管理增加、删除和调整VLAN时，会自动地将信息向网络中其他的交换机广播。另外，VTP减小了那些可能导致安全问题的配置，便于管理，只要在VTP Server上做相应设置，VTP Client会自动学习VTP Server上的VLAN信息。

使用VTP功能，必须配置VTP域，一是域内的每台交换机都必须使用相同的域名，不论是通过配置实现，还是由交换自动学到的；二是交换机必须是相邻的，即相邻的交换机需要具有相同的域名；三是在所有交换机之间，必须配置中继链路。如果上述3个条件任何一项不满足，则VTP域不能联通，信息也就无法跨越分离部分进行传送。

VTP有3种工作模式：VTP Server、VTP Client 和 VTP Transparent。一般，一个VTP域内的整个网络只设一个VTP Server。VTP Server维护该VTP域中所有VLAN 信息列表，VTP Server可以建立、删除或修改VLAN，发送并转发相关的通告信息，同步VLAN配置，会把配置保存在NVRAM中。VTP Client虽然也维护所有VLAN信息列表，但其VLAN的配置信息是从VTP Server学到的，VTP Client不能建立、删除或修改VLAN，但可以转发通告，同步VLAN配置，不保存配置到NVRAM中。VTP Transparent相当于是一台独立的交换机，它不参与VTP工作，不从VTP Server上学习VLAN的配置信息，而只拥有本设备上自己维护的VLAN信息。VTP3种模式的区别和联系如表2-1所示：

表2-1　VTP3种模式的区别和联系

模式名称 / 功能	Server模式	Client模式	Transparent模式
创建VLAN	√	×	√
修改VLAN	√	×	√
删除VLAN	√	×	√
发送设定给其他设备做同步	√	×	×
转发设定给其他设备	√	√	√
同步其他设备给的VLAN设定	√	√	×
VLAN信息存储于NVRAM	√	×	√

2.2 运维实例：用最简单网络学习二、三层协议

计算机网络知识的学习，离不开多次试验的实践学习。但昂贵的网络设备，对许多想搭建真实网络环境的人又望而却步。不过，现在我们借助简单的设备搭建所需的网络环境也完全是有可能的。下面的一个实例所需的设备就非常少，只需两台电脑和一根交叉网线即可。若你觉得具备这些设备还是有些困难，那只用一台电脑也完全可以，只需在网上下载一个VMware虚拟机软件，安装后进行相应的设置，就可以进行下面的实例学习。

不过下面提到的命令和参数，都是在有两台电脑的实验环境中完成的。操作系统使用的是Win7，两台电脑都没有配置默认网关。还需要注意的就是连接两台电脑用的是交叉网线，网线一端是T568A标准的线序，另一端是T568B标准的线序，不能使用直通线。下面就一步步介绍实验过程中碰到的问题和解决问题的方法，期间也就很自然地学习了TCP/IP协议族中的二、三层协议。

1. 搭建环境

如图2-1所示，这种实验环境很简单，想必大家都试验过。它也很容易理解，处在同一网络中的两台PC，不用配置网关，也能够互相通信。

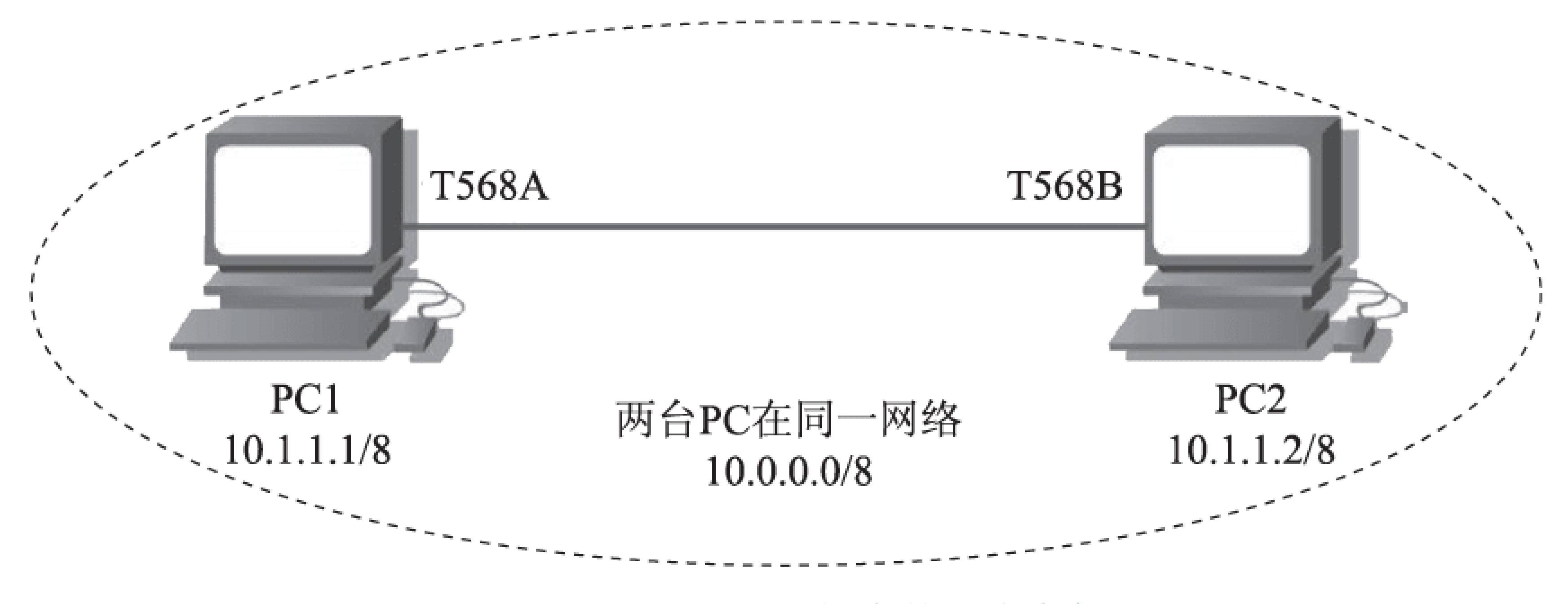


图2-1　位于同一网络中的两台主机

2. 深入操作

如图2-2所示，两台PC在不同的网络中，但还要让PC1和PC2之间能互相ping通。这种网络实验环境，可能很多人没有深入研究过，下面就通过一些实验截图

一步步分析。

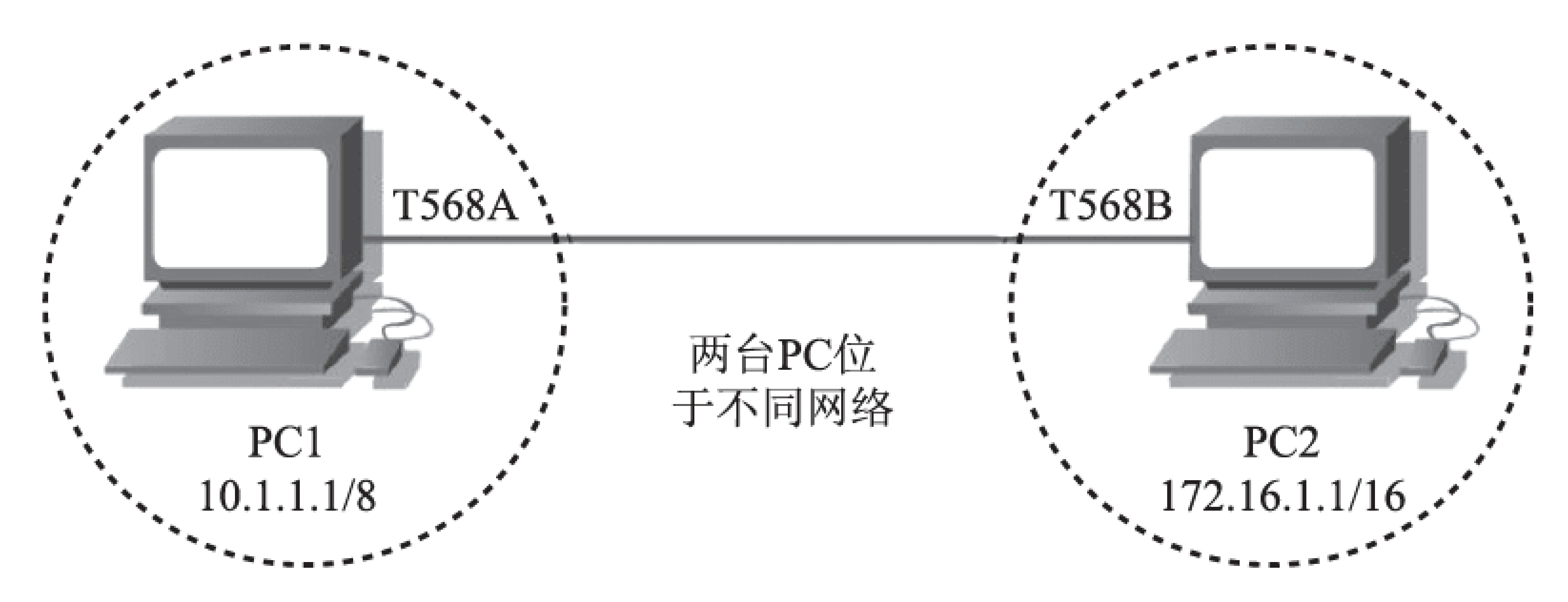


图2-2　位于不同网络中的两台主机

(1)如图2-3所示，在PC1上ping主机PC2是不通的。若能保证连接两台PC的网线没有故障，ping不通的话，问题肯定首先出在PC1的路由上。

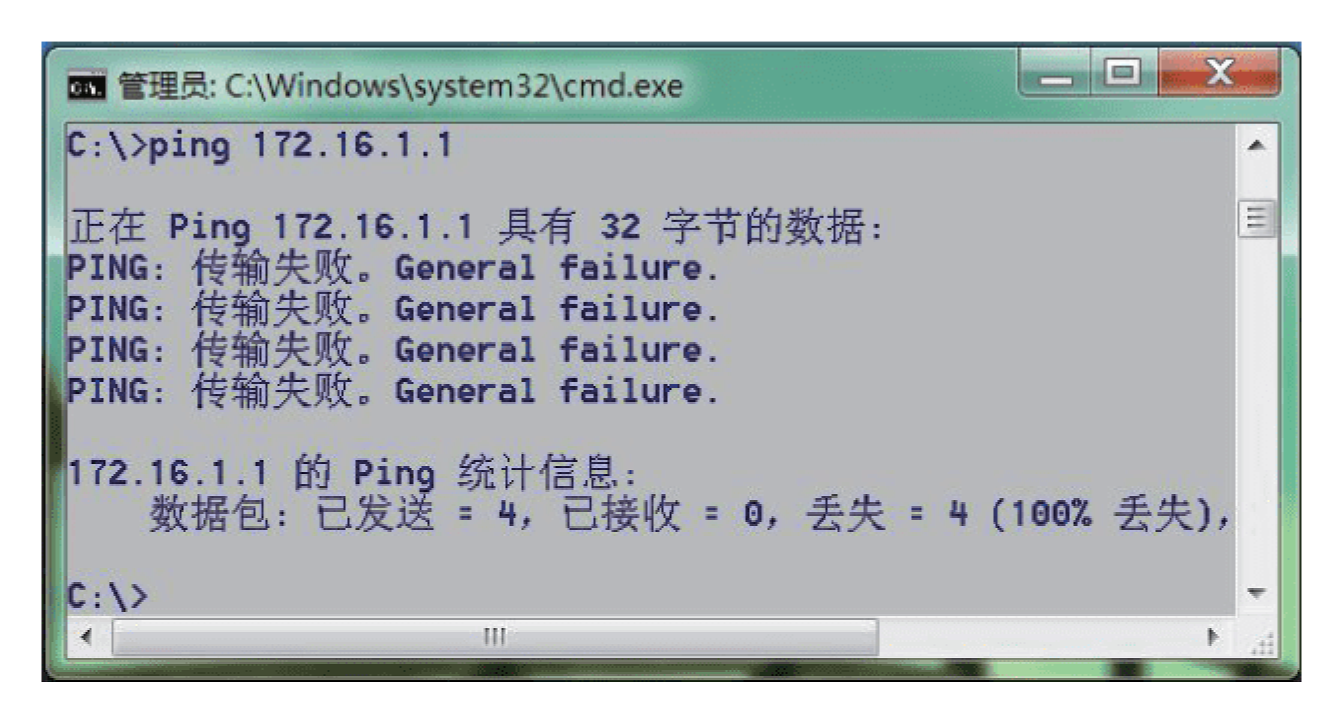


图2-3　PC1不能ping通PC2

(2)如图2-4所示，在PC1的“命令行”中，执行“route print”命令，就能看到PC1主机上的路由表，在其中看不到到达目的网络172.16.0.0/16的路由。所以，在PC1上执行ping 172.16.1.1命令后，PC1首先在它的路由表中查找有没有到达网络172.16.0.0/16的路由表项，若没有就会返回如图2-3所示的结果。

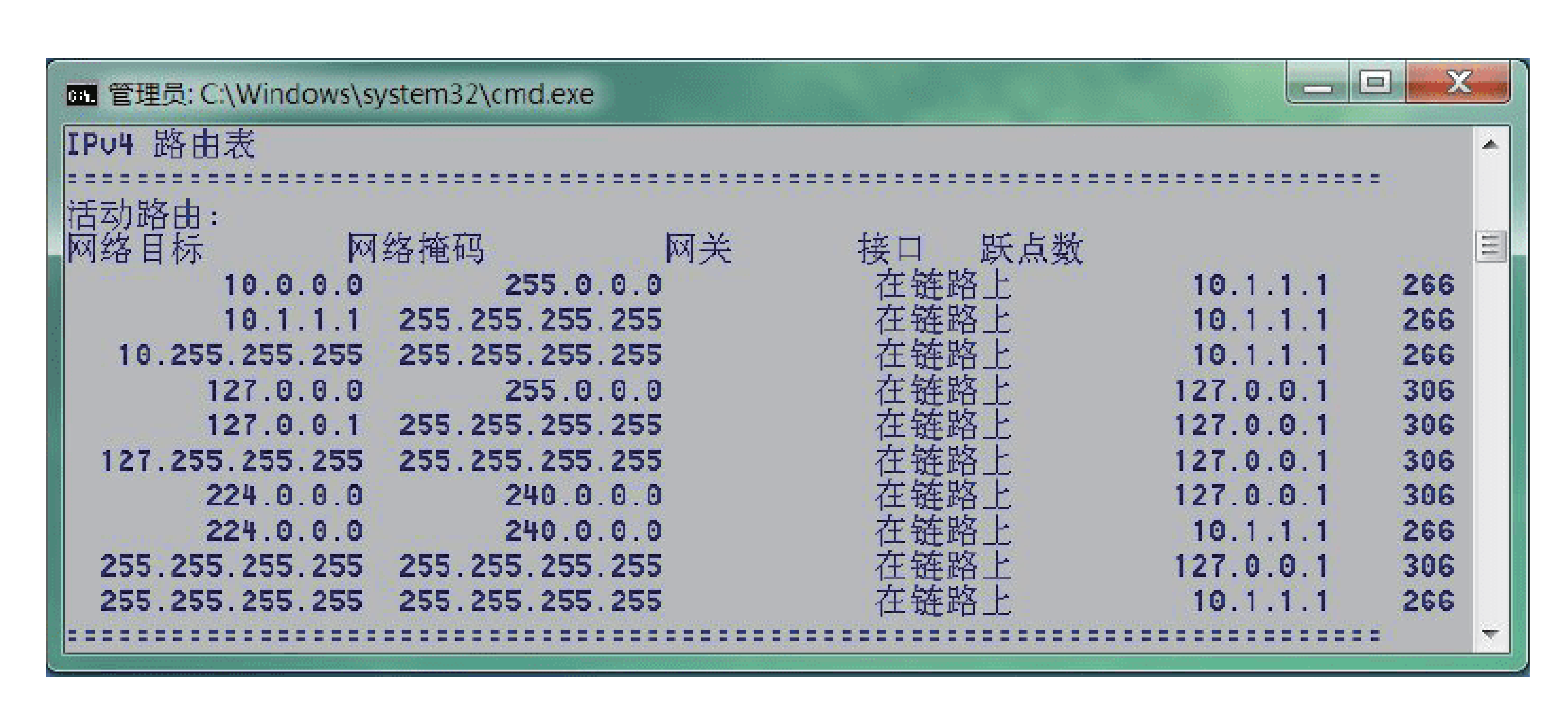


图2-4　主机PC1中的路由表

(3)既然路由表中没有到网络172.16.0.0/16的路由，那PC1中的二层ARP表中有没有与172.16.1.1对应的MAC地址表项呢？因为只有IP地址和MAC地址之间进行了一一对应的绑定，主机在封装完三层具有源和目的IP地址的数据包后，然后在进行二层封装数据帧时，必须找到与IP目的地址对应的MAC地址，才能完成二层的封装。不过如图2-5所示，PC1中的ARP表中，并没有IP地址172.16.1.1和PC2的MAC地址的对照表。

```
管理员: C:\Windows\system32\cmd.exe
C:\>arp -a

接口: 10.1.1.1 --- 0xc
  Internet 地址         物理地址              类型
  10.255.255.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态

C:\>
```

图2-5　主机PC1中的ARP表

(4)既然PC1的路由表中没有到网络172.16.0.0/16的路由，那就在PC1中添加一条静态路由，如图2-6所示。注意添加静态路由的命令格式，必须和图2-6所示的一致。只是在命令的最后还有一个“IF”参数，可以省略不写，这并不影响命令的正确执行。

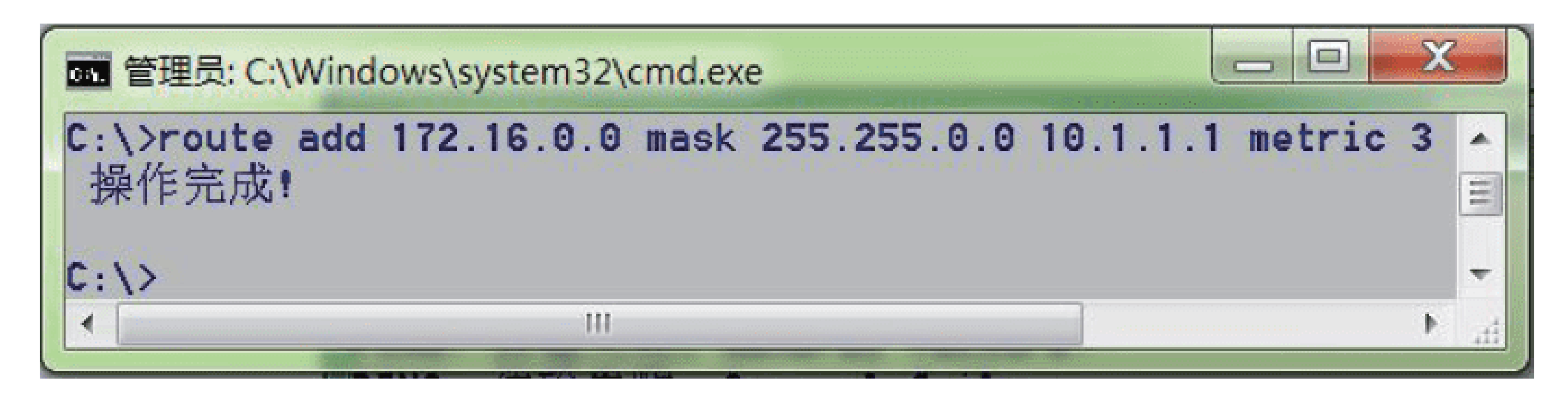


图2-6　在主机PC1中添加静态路由

(5)执行完添加静态路由的命令后，在PC1中再次执行命令“route print”后，发现PC1的路由表中，已经包含了到网络172.16.0.0/16的路由，如图2-7所示。

(6)既然PC1中的路由表中已经包括了到达网络172.16.0.0/16的路由，那是不是在PC1上就能ping通172.16.1.1了？结果如图2-8所示，这时PC1还是不能ping通PC2。

```
管理员: C:\Windows\system32\cmd.exe
IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口    跃点数
        10.0.0.0        255.0.0.0            在链路上         10.1.1.1    266
        10.1.1.1  255.255.255.255            在链路上         10.1.1.1    266
  10.255.255.255  255.255.255.255            在链路上         10.1.1.1    266
       127.0.0.0        255.0.0.0            在链路上        127.0.0.1    306
       127.0.0.1  255.255.255.255            在链路上        127.0.0.1    306
 127.255.255.255  255.255.255.255            在链路上        127.0.0.1    306
      172.16.0.0      255.255.0.0            在链路上         10.1.1.1     13
   172.16.255.255  255.255.255.255           在链路上         10.1.1.1    266
       224.0.0.0        240.0.0.0            在链路上        127.0.0.1    306
       224.0.0.0        240.0.0.0            在链路上         10.1.1.1    266
 255.255.255.255  255.255.255.255            在链路上        127.0.0.1    306
 255.255.255.255  255.255.255.255            在链路上         10.1.1.1    266
===========================================================================
```

图2-7　PC1路由表中包含了到PC2网络的路由



图2-8　在主机PC1上还是ping不通PC2

这是因为，虽然PC1路由表中包含有到PC2的路由，这样在PC1上发送具有目的IP地址是172.16.1.1的ping包时，数据包能够到达PC2。但是当PC2收到ping包后，PC2依据ping的性质，还要把ping包再发送回PC1，在PC1收到PC2返回的ping包后，一个完整的ping过程才结束。

但是当PC2发送ping包前，它在自己的路由表中要查找，有没有到达目的网络地址是10.0.0.0/8的路由，但是它没有找到这项路由。在这种情况下PC2就自动丢弃了这个ping包，所以PC1也就收不到由PC2返回的ping包，自然也就有了图2-8所示的结果。

(7)不过这时在PC1上，也发生了一个明显的变化。当再次在命令行中执行命令“arp -a”后，发现PC1的ARP表中多了一项IP地址172.16.1.1和PC2的MAC地址的绑定项，如图2-9所示。

```
管理员: C:\Windows\system32\cmd.exe
C:\>arp -a

接口: 10.1.1.1 --- 0xc
  Internet 地址         物理地址              类型
  10.255.255.255        ff-ff-ff-ff-ff-ff     静态
  172.16.1.1            00-23-8b-d5-96-be     动态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态

C:\>
```

图2-9 PC1中已有了包含PC2的ARP表项

这是因为，当在PC1上执行“ping 172.16.1.1”命令后，PC1首先在路由表中找到了到达网络172.16.0.0/16的路由表项，然后就对数据包进行三层封装。当三层封装完成后，PC1就要根据172.16.1.1对应的MAC地址，对数据包进行二层封装。这是因为只有把正确的MAC地址封装进数据帧后，数据包才能在以太网中被正确地送达目的地，因为在以太网中只依据二层MAC地址，而不是三层IP地址传输数据。但这时当PC1在ARP表中查找172.16.1.1的MAC地址时，它并没有找到。

这时PC1就会发出一个广播包，询问谁有IP地址172.16.1.1的MAC地址，当PC2收到这个广播包后，发现172.16.1.1这个IP地址和自己的IP地址一样，就给PC1返回一个数据包，数据包中就包括有和172.16.1.1对应的MAC地址，当PC1收到这个数据包后，就会在自己的ARP表中添加与IP地址172.16.1.1对应的MAC地址表项，所以当再次执行“arp -a”命令后，就能看到多了这一项。

那为什么第一次执行“arp -a”命令时，PC1的ARP表中没有与172.16.1.1对应的MAC地址绑定呢？因为第一次在PC1上执行ping 172.16.1.1命令时，PC1在路由表中没有找到与网络172.16.0.0/16对应的路由，这时PC1就自动放弃了封装三层数据包的行为，既然三层数据包都没有进行封装，就更谈不上在PC1中进行二层封装了，所以PC1也就没有必要知道与172.16.1.1对应的MAC地址了，也就没有再发送一个广播包询问与172.16.1.1对应的MAC地址。所以，第一次执行“arp -a”命令时，PC1的ARP表中并没有与172.16.1.1对应的MAC地址表项。

(8)既然现在知道在PC1上ping不通PC2是因为在PC2上没有到达网络10.0.0.0/8的路由，那现在就在PC2上添加一条静态路由，如图2-10所示，格式和

在PC1上添加到网络172.16.0.0/16的路由格式是一样的。

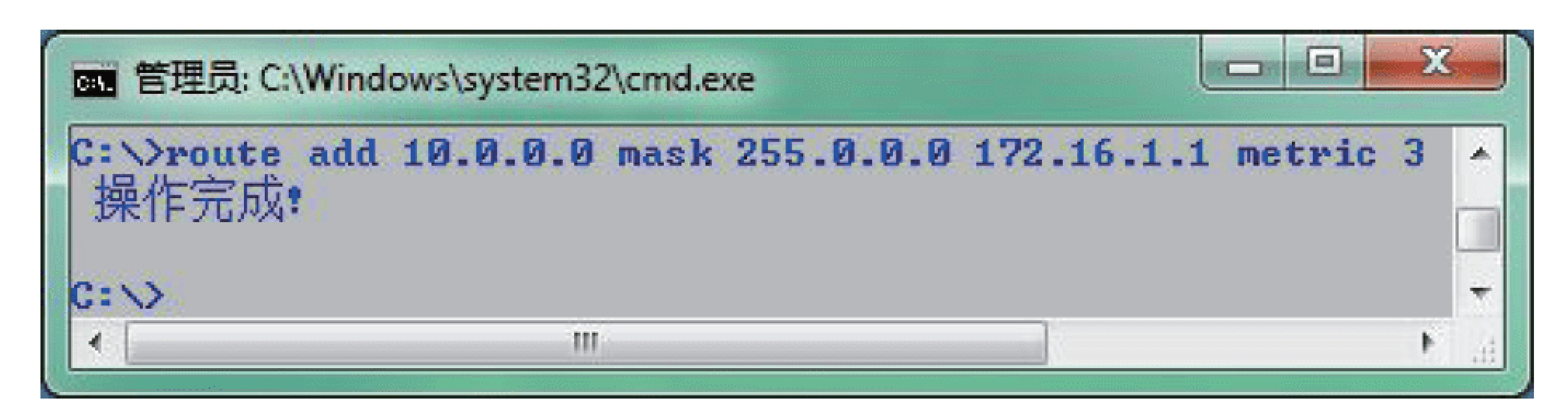


图2-10　在主机PC2上添加静态路由

(9)在PC2上添加完静态路由后，再在PC1上执行ping命令后，就能ping通了，如图2-11所示。因为ping包到达PC2后，也能在路由表中找到去往PC1网络10.0.0.0/8的路由了。

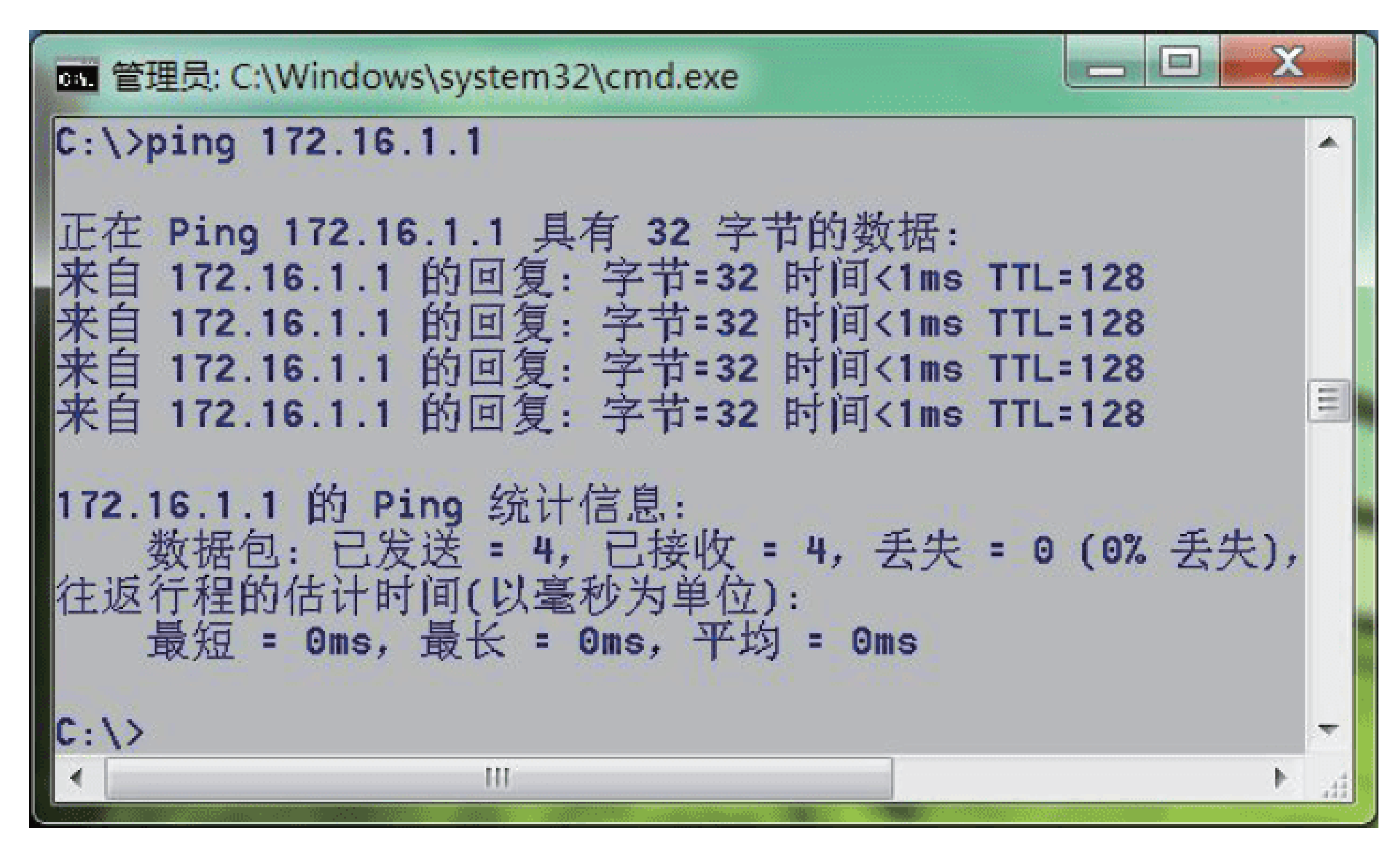


图2-11　在PC1上能够ping通PC2

3. 总结

1)ARP(Address Resolution Protocol，地址解析协议)

(1)概念：ARP工作在数据链路层，它和硬件接口进行联系，同时对上层提供服务。ARP将计算机的32位网络IP地址，转化为48位的MAC物理地址。在以太网中的数据帧从一个主机到达网内的另一台主机是根据48位的以太网地址来确定接口的，而不是根据32位的IP地址。计算机网卡的驱动程序，必须知道目的端的硬件MAC地址才能发送数据。因此，必须把IP目的地址转换成以太网的目的地址。

在TCP/IP协议栈中，网络层和传输层只关心目标主机的IP地址。这就导致

在以太网中使用IP协议时，数据链路层的以太网协议接到上层IP协议提供的数据中，只包含目的主机的IP地址。而地址解析(address resolution)就是主机在发送数据帧前将目标IP地址转换成目标MAC地址的过程。ARP在正常情况下的通信模式应该是：请求→应答→请求→应答，也就是一问一答的规则。

(2)ARP工作原理：首先，每台主机都会在自己的ARP缓冲区中建立一个ARP列表，以表示IP地址和MAC地址之间的对应关系。当源主机需要将一个数据包发送到目的主机时，会首先检查自己 ARP列表中是否存在该 IP地址对应的MAC地址，如果有，就直接将数据包发送到这个MAC地址。如果没有，就向本地网段发起一个ARP请求的广播包，查询此目的主机对应的MAC地址。此ARP请求数据包里包括源主机的IP地址、硬件地址及目的主机的IP地址。网络中所有的主机收到这个ARP请求后，会检查数据包中的目的IP是否和自己的IP地址一致。如果不相同就忽略此数据包；如果相同，该主机首先将发送端的MAC地址和IP地址添加到自己的ARP列表中，如果ARP表中已经存在该IP的信息，则将其覆盖，然后给源主机发送一个 ARP响应数据包，告诉对方自己是它需要查找的MAC地址。源主机收到这个ARP响应数据包后，将得到的目的主机的IP地址和MAC地址添加到自己的ARP列表中，并利用此信息开始数据的传输。如果源主机一直没有收到ARP响应的数据包，就表示ARP查询失败。

(3)ARP攻击：是通过伪造IP地址和MAC地址，实现ARP欺骗。ARP攻击能够在网络中产生大量的ARP通信，从而使网络阻塞。攻击者只要持续不断的发出伪造的ARP响应包就能更改目标主机ARP缓存中的IP-MAC条目，从而造成网络中断或中间人攻击。

2)理解路由的两个关键知识点

(1)路由器对三层数据包的路由转发，是根据“网络地址”转发数据包的，而不是根据“IP地址”转发的。例如，一台路由器收到一个需要路由的数据包，数据包的目的IP地址是213.17.53.9，掩码是255.255.255.0。然后路由器首先要做的是结合数据包的IP地址和掩码，算出数据包要被路由的目的网络地址是213.17.53.0/24，然后，路由器才会在其路由表中查找有没有到网络213.17.53.0/24的路由，而不是查找到IP地址213.17.53.9的路由，若有就依据路由表提供的信息，在相应的接口上将数据包转发出去。若没有找到对应的路由，则路由器就会自动把数据包丢弃。

(2)路由器对数据包的路由是依据三层数据包中的“目的IP地址”进行路由转发的，而和数据包中的“源IP地址”没有关系。也就是路由器收到三层数据包后，只需要数据包中的目的IP地址和目的IP地址的掩码就可完成对数据包的路由，整个过程没有使用到三层数据包中的源IP地址及其掩码。

2.3 运维实例：实例解析GVRP、VTP协议和Trunk技术

GVRP、VTP协议和Trunk技术三者之间有很多的相似性：它们都属于二层协议或二层技术；在这三者的具体配置命令中，涉及最多的配置就是VLAN方面的配置；三者的广泛应用都是为了精简网络维护人员在配置和管理网络设备时对命令频繁和大量的使用。但它们之间又有着根本的不同，下面就以3则实例，分别对其进行全面的介绍。

1. GVRP在H3C交换机上的应用

GVRP(GARP VLAN Registration Protocol，GARP VLAN注册协议)是GARP(Generic Attribute Registration Protocol，通用属性注册协议)的一种应用。GARP的应用主要包括GMRP和GVRP，其中GMRP(GARP Multicast Registration Protocol，GARP组播注册协议)是基于GARP的一个组播注册协议。用于维护交换机中的组播注册信息。而GVRP维护设备中的VLAN 动态注册信息，并传播该信息到其他的设备中。

设备启动 GVRP 特性后，能够接收来自其他设备的VLAN 注册信息，并动态更新本地的VLAN 注册信息，包括当前的VLAN 成员、这些VLAN 成员可以通过哪个端口到达等。而且设备能够将本地的VLAN 注册信息向其他设备传播，以便使同一局域网内所有设备的VLAN 信息达成一致。GVRP 传播的VLAN 注册信息既包括本地手工配置的静态注册信息，也包括来自其他设备的动态注册信息。下面就通过一则实例介绍GVRP协议在H3C交换机上的应用。

如图2-12所示，3台交换机的型号都是H3C S3100-52TP-SI，两两互联。设备

间的连接情况如下所示：

```
S3100-A Eth 1/0/1 <-----> S3100-B Eth 1/0/1
S3100-B Eth 1/0/2 <-----> S3100-C Eth 1/0/1
S3100-C Eth 1/0/2 <-----> S3100-A Eth 1/0/2
```

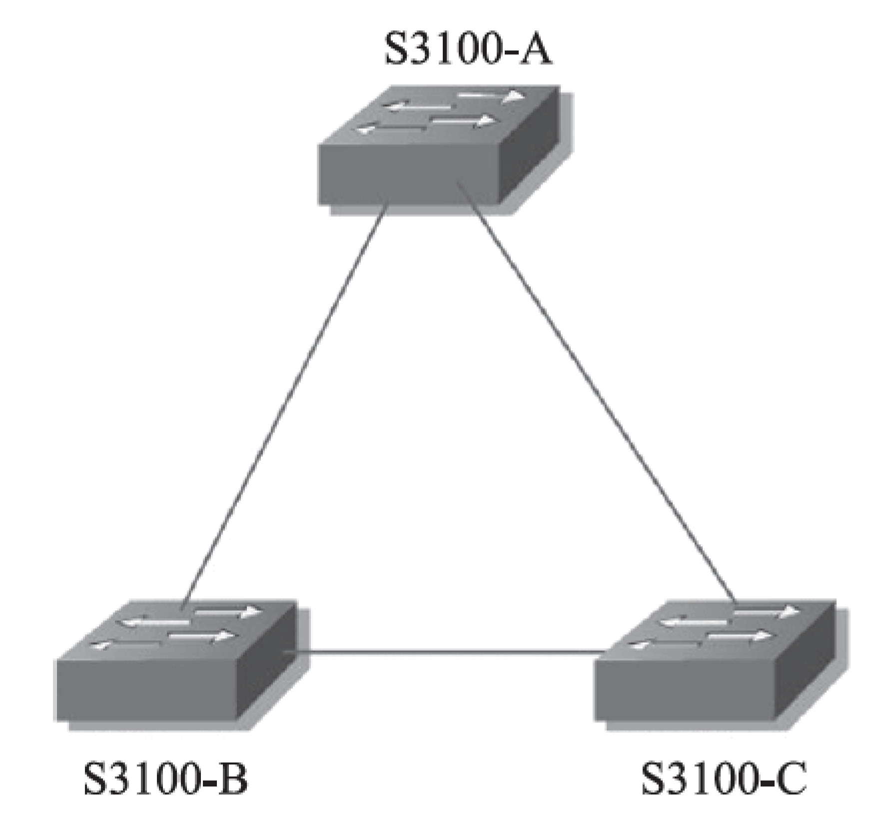


图2-12　3个H3C S3100交换机两两互联图示

在S3100-A上的配置如下所示：

```
[S3100-A] gvrp
//开启全局GVRP功能，缺省情况下，全局GVRP功能处于关闭状态
[S3100-A] interface ethernet 1/0/1
[S3100-A-Ethernet1/0/1] port link-type trunk
[S3100-A-Ethernet1/0/1] port trunk permit VLAN all
[S3100-A] interface ethernet 1/0/2
[S3100-A-Ethernet1/0/2] port link-type trunk
[S3100-A-Ethernet1/0/2] port trunk permit VLAN all
//将两个以太网端口Ethernet1/0/1和Ethernet1/0/2 配置为Trunk
```

```
端口，并允许所有VLAN 通过
    [S3100-A-Ethernet1/0/1] gvrp
    [S3100-A-Ethernet1/0/2] gvrp
    //在两个Trunk 端口上开启GVRP功能，缺省情况下，端口GVRP 功能处于关闭状态
    [S3100-A] VLAN 2
    //配置静态VLAN 2
```

在S3100-B上的配置如下所示：

```
    [S3100-B] gvrp
    //开启全局GVRP功能
    [S3100-B] interface ethernet 1/0/1
    [S3100-B-Ethernet1/0/1] port link-type trunk
    [S3100-B-Ethernet1/0/1] port trunk permit VLAN all
    [S3100-B] interface ethernet 1/0/2
    [S3100-B-Ethernet1/0/2] port link-type trunk
    [S3100-B-Ethernet1/0/2] port trunk permit VLAN all
    //将两个以太网端口Ethernet1/0/1和Ethernet1/0/2 配置为Trunk端口，并允许所有VLAN 通过
    [S3100-B-Ethernet1/0/1] gvrp
    [S3100-B-Ethernet1/0/2] gvrp
    //在两个Trunk 端口上开启GVRP功能
    [S3100-B-Ethernet1/0/2] gvrp registration fixed
    //配置端口注册模式为Fixed，缺省情况下，GVRP 端口注册模式为Normal
```

```
[S3100-B] VLAN 3
//配置静态VLAN 3
```

在S3100-C上的配置如下所示：

```
[S3100-C] gvrp
//开启全局GVRP功能
[S3100-C] interface ethernet 1/0/1
[S3100-C-Ethernet1/0/1] port link-type trunk
[S3100-C-Ethernet1/0/1] port trunk permit VLAN all
[S3100-C] interface ethernet 1/0/2
[S3100-C-Ethernet1/0/2] port link-type trunk
[S3100-C-Ethernet1/0/2] port trunk permit VLAN all
//将两个以太网端口Ethernet1/0/1和Ethernet1/0/2 配置为Trunk
端口，并允许所有VLAN 通过
[S3100-C-Ethernet1/0/1] gvrp
[S3100-C-Ethernet1/0/2] gvrp
//在Trunk 端口上开启GVRP功能
[S3100-C-Ethernet1/0/1] gvrp registration forbidden
[S3100-C-Ethernet1/0/2] gvrp registration forbidden
//配置两个端口的注册模式都为Forbidden
[S3100-C] VLAN 4
//配置静态VLAN4
```

以上3个H3C交换机上的配置命令看着好像都一样，但其实在最关键的地方都会有细微的差别。主要就是在配置端口的注册模式时，3个交换机上端口的配置是不一样的。S3100-A的两个端口上没有专门配置注册模式，但默认情况下使用的就是Normal模式，所以S3100-A的Ethernet1/0/1和Ethernet1/0/2的端口注册模式为Normal；S3100-B上的Ethernet1/0/1也没有专门配置注册模式，所以它也是Normal模式，而S3100-B的Ethernet1/0/2端口注册模式配置成了Fixed模式；S3100-C上的两个端口配置成了Forbidden模式。所以这几个端口在实际的运行中，所传播VLAN的机制会有所不同。

可以使用命令“display VLAN dynamic”来查看验证各个端口的运行机制，命令中的dynamic参数是指显示系统动态创建的VLAN的数量和编号，动态VLAN是指通过GVRP协议生成或通过Radius服务器所下发的VLAN。下面是在3台交换机上分别执行“display VLAN dynamic”的显示结果：

```
[S3100-A] display VLAN dynamic
Now, the following dynamic VLAN exist(s):
3
//显示S3100-A上的动态VLAN 信息
[S3100-B] display VLAN dynamic
Now, the following dynamic VLAN exist(s):
2
//显示S3100-B上的动态VLAN 信息
[S3100-C] display VLAN dynamic
Now, the following dynamic VLAN exist(s):
No dynamic VLANs exist!
//显示S3100-C上的动态VLAN 信息
```

从以上的输出结果可以看出，S3100-A和S3100-B两台交换机之间可以互相交换所创建的VLAN，这是因为S3100-A的Ethernet1/0/1和S3100-B的Ethernet1/0/1

端口的注册模式都是Normal模式，此模式允许端口动态注册、传播动态VLAN以及静态VLAN 信息。但是在S3100-A和S3100-B两台交换机上看不到S3100-C交换机所创建的VLAN 4，同时在S3100-C上也看不到S3100-A和S3100-B两台交换机所创建的VLAN 2和VLAN 3信息，这是因为虽然分别在S3100-A和S3100-B的Ethernet1/0/2端口上配置了Normal和Fixed模式，但S3100-C两个端口的注册模式都是Forbidden，所以S3100-C和其他两台交换机之间也就不能交换除VLAN 1以外的所有VLAN信息。GVRP的端口注册模式有以下3种：

Normal模式：允许该端口动态注册、注销VLAN、传播动态VLAN 以及静态VLAN 信息。

Fixed模式：禁止该端口动态注册、注销VLAN，只传播静态VLAN 信息，不传播动态VLAN 信息。也就是说被设置为Fixed 模式的Trunk 口，即使允许所有VLAN 通过，实际通过的VLAN 也只能是手动配置的那部分。

Forbidden模式：禁止该端口动态注册、注销VLAN，不传播除VLAN1 以外的任何的VLAN 信息。也就是说被配置为Forbidden 模式的Trunk 端口，即使允许所有VLAN 通过，实际通过的VLAN也只能是VLAN1。

另外，可以通过一些“display gvrp”命令显示配置后GVRP的运行情况，或者是查看显示信息验证配置效果。命令如下所示：

```
[H3C-S3100]display gvrp status
//显示GVRP 的全局状态信息
[H3C-S3100]display gvrp statistics [ interface interface-list ]
//显示 GVRP 的统计信息
[H3C-S3100]display gvrp state interface interface-type interface-number VLAN VLAN-id
//显示 GVRP 的状态机信息
[H3C-S3100]display gvrp VLAN-operation interface interface-type interface-number
//显示当前的动态 VLAN 操作信息
```

2. Trunk技术在Cisco交换机和H3C交换机之间的应用

从上面的例“1”中，可以看出GVRP协议可以减轻网络维护人员在进行网络设备二层配置方面的工作量。可能在配置几个或十几个VLAN时感觉不出GVRP的作用所在，但如果要配置的VLAN数量在成百上千的话，马上就能体现出GVRP的巨大功用。只需要在一台设备上配置好相关的VLAN，其他的设备只要设置好GVRP的相关设置，它就会自动把VLAN的配置同步过去。

但是，所有协议的使用都只能在支持它的设备上使用，GVRP协议在以前思科的CatOS系统上支持的还比较好。目前，大部分的思科IOS系统已不支持GVRP协议。而目前H3C的设备基本上都能支持GVRP协议。所以在实际工作中，如果使用的网络设备都是思科的设备，或者所有的设备都是H3C设备，就可以使用VTP或GVRP协议简化网络的配置工作。但若是思科的设备和H3C的设备放在一起使用话，GVRP协议和VRP协议就不能再应用了。如图2-13所示，一台Cisco3750交换机和一台H3C S3100相连，它们相连的端口分别为Cisco3750 GigabitEthernet1/0/1和H3C S3100 GigabitEthernet1/1/1。



图2-13　Cisco3750和H3C S3100交换机相连图示

为了让两台交换机中的VLAN数据能够互相通信，最好的方法就是使用Trunk技术。如下所示是在H3C和Cisco交换机上所做的Trunk配置：

```
[H3C-S3100] interface GigabitEthernet1/1/1
[H3C-S3100-GigabitEthernet1/1/1] port link-type trunk
[H3C-S3100-GigabitEthernet1/1/1] port trunk permit VLAN all
//把H3C-S3100的GigabitEthernet 1/1/1端口配置为trunk模式，并允许所有VLAN通过
Cisco3750(config)#interface GigabitEthernet1/0/1
```

```
Cisco3750(config-if)# switchport trunk encapsulation dot1q
Cisco3750(config-if)#switchport trunk allowed VLAN all
Cisco3750(config-if)#switchport mode trunk
//把Cisco3750的Gig1/0/1端口配置为Trunk模式，并指定封装模式为dot1q
```

在进行上面的配置命令时，在Cisco的交换机上最好指定Trunk的封装模式，因为默认情况下，思科设备使用的封装模式可能是思科专有的封装模式ISL。而H3C交换机只支持dot1q的封装模式，所以双方必须匹配才行。配置完上面的命令后，也可以使用如下所示的命令，查看在端口上配置的Trunk情况：

```
Cisco3750#show interface trunk
Port     Mode     Encapsulation  Status      Native VLAN
Gi1/0/1      on         802.1q        trunking        1

Port         VLANs allowed on trunk
Gi1/0/1         1-4094
//在Cisco3750上查看显示的结果
[H3C-S3100]display port trunk
 The following trunk ports exist:
  GigabitEthernet1/1/1
//在H3C S3100上查看显示的结果
```

通过上面的查看命令可以确定，在两个交换机上的两个端口上已做好了Trunk的配置。这时只要在两台交换机上分别创建相同的VLAN，并把Cisco3750

和H3C S3100交换机上的其他端口都划入到所创建的VLAN中，并在两个交换机上分别接入两个终端，并在终端上配置相应的IP地址，这样两个终端就可以通过两个交换机进行通信了。例如，在两台交换机上都创建了VLAN 2，并把Cisco3750的Gi1/0/2和H3C S3100的Eth1/0/1都划入到VLAN 2中，然后分别在这两个端口上接入PC1和PC2，PC1的IP地址为192.168.2.1 255.255.255.0，PC2的IP地址为192.168.2.2 255.255.255.0，这样在PC1上就能ping通PC2的IP地址192.168.2.2，同理PC2也能ping通PC1。

通过上面的配置，使用Trunk技术也就很好地解决了不同型号网络设备之间的数据通信。

3. VTP协议在Cisco交换机上的应用

VTP(VLAN Trunking Protocol)协议是思科私有协议，它的作用和上面提到的GVRP协议基本一致。如图2-14所示，网络中共使用了4台Cisco3750交换机，设备间的连接情况如下所示：

```
3750-A GigabitEthernet 1/0/1 <-----> 3750-C GigabitEthernet 1/0/1
3750-A GigabitEthernet 1/0/2 <-----> 3750-B GigabitEthernet 1/0/1
3750-B GigabitEthernet 1/0/2 <-----> 3750-D GigabitEthernet 1/0/2
3750-C GigabitEthernet 1/0/2 <-----> 3750-D GigabitEthernet 1/0/1
```

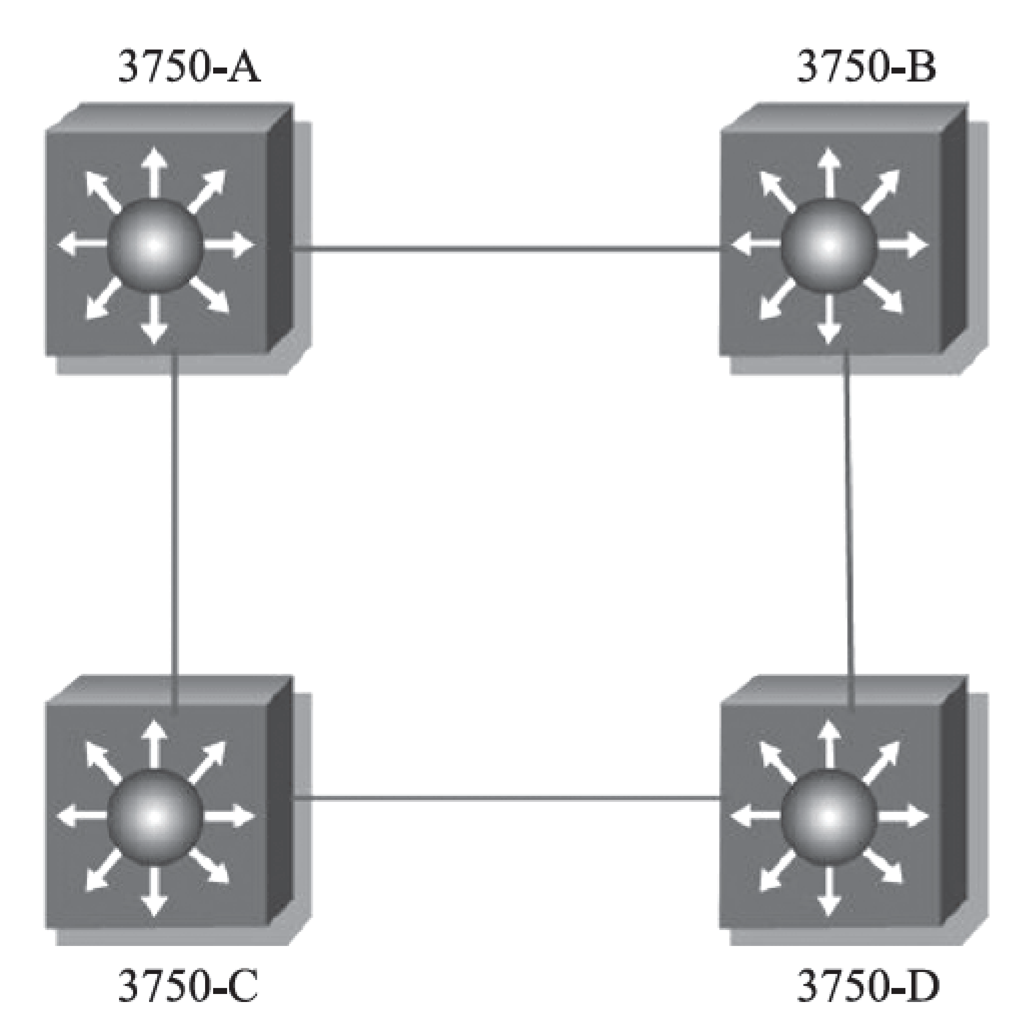


图2-14　4个Cisco3750交换机通过Trunk线相连图示

网络中的四4条线路都是Trunk线路，每台交换机上的两个端口都配置成了Trunk口，其中3750-A上的两个端口的配置如下所示：

```
3750-A(config)#interface GigabitEthernet1/0/1
3750-A(config-if)# switchport trunk encapsulation dot1q
3750-A(config-if)#switchport trunk allowed VLAN all
3750-A(config-if)#switchport mode trunk
3750-A(config)#interface GigabitEthernet1/0/2
3750-A(config-if)# switchport trunk encapsulation dot1q
3750-A(config-if)#switchport trunk allowed VLAN all
3750-A(config-if)#switchport mode trunk
```

然后在3750-B、3750-C和3750-D3台交换机上共6个端口上的Trunk配置命令和上面在3750-A上两个端口的配置命令是一样的。

下面是在4台Cisco3750交换机上配置VTP的命令：

```
3750-A(config)#vtp version 2
3750-A(config)#vtp domain cisco
3750-A(config)#vtp password 123456
3750-A(config)#vtp mode server
//在3750-A上配置VTP，并把VTP模式配置为server
3750-B(config)#vtp version 2
3750-B(config)#vtp domain cisco
3750-B(config)#vtp password 123456
3750-B(config)#vtp mode client
//在3750-B上配置VTP，并把VTP模式配置为client
3750-C(config)#vtp version 2
3750-C(config)#vtp domain cisco
3750-C(config)#vtp password 123456
3750-C(config)#vtp mode client
//在3750-C上配置VTP，并把VTP模式配置为client
3750-D(config)#vtp version 2
3750-D(config)#vtp domain cisco
3750-D(config)#vtp password 123456
3750-D(config)#vtp mode transparent
//在3750-D上配置VTP，并把VTP模式配置为transparent
```

在进行上面的配置时需要注意，所有交换机必须使用相同的VTP域名，除非网络设计时就强调了多个不同的VTP域；在同一个VTP域中，所有的交换机都必须运行同一个VTP版本；在同一个VTP域中，在交换机上配置VTP密码并不是必须的，但如果要使用VTP密码，所有的交换机就必须使用相同的VTP密码；所有

VTP服务器模式的交换机都应具有相同的配置修改编号，而且应当是在最高编号的域中；在必须把一个交换机从透明模式转换成服务器模式时，先要把透明模式交换机上的所有VLAN退出服务器模式。

配置完上面的命令后，就可以在VTP模式是server的3750-A上创建VLAN，然后所创建的VLAN会自动分发到3750-B和3750-C上。也就是在3750-B和3750-C上不用手动创建VLAN，它们上面就会自动生成在3750-A上所创建的VLAN。例如，在3750-A上创建了VLAN 2， 那么在3750-B和3750-C上，使用命令“show VLAN”，就能查看到在这两个交换机上也存在VLAN 2。但是在3750-D上就查看不到存在VLAN 2的信息。

这是因为3750-A 的VTP模式是server模式，它可以维护该VTP域中所有VLAN 信息列表，可以创建、删除或修改VLAN。而3750-B和3750-C 的VTP模式是client模式，它虽然也维护所有VLAN信息列表，但其VLAN的配置信息是从3750-A学到的。VTP Client不能建立、删除或修改VLAN。另外，3750-D的VTP模式是Transparent，它相当于是网络中一台独立的交换机，不参与VTP的工作，它不从VTP Server学习VLAN的配置信息，它只拥有本交换机上自己维护的VLAN信息。3750-D只可以创建、删除和修改本机上的VLAN信息。

可以使用命令“show vtp status”查看交换机上配置VTP的基本信息，如下所示是在3750-A上执行此命令的输出：

```
3750-A#show vtp status
VTP Version                      : 2
Configuration Revision             : 6
Maximum VLANs supported locally    : 1005
Number of existing VLANs           : 1
VTP Operating Mode               : Server
VTP Domain Name                 : cisco
```

从上面所配置的命令可以看出，如果把3750-A、3750-B和3750-C上还没有使用的端口都划入到VLAN 2中，那接入到所有这些端口上的终端之间就可以通信了，因为这些终端实际上都是位于VLAN 2的这个局域网中。但是如果想让连接到VTP模式是Transparent的3750-D上的终端，也能和连接到3750-A上的位于VLAN 2中的终端之间相互通信，那还需要做那些配置？

因为3750-D交换机VTP模式的缘故，它上面并没有自动创建VLAN 2，不过这时我们可以在3750-D上手动创建VLAN 2，又因为3750-D与两个交换机3750-B和3750-C的连接都是Trunk连接，并且允许所有VLAN在其上通过。所以，只要在3750-D上手动创建了VLAN 2，并把3750-D上没有使用的端口都划入到VLAN 2中，这样接入到位于3750-D上VLAN 2中端口的终端，也就能和接入到3750-A上VLAN 2中端口的终端之间相互通信了。

但这时图2-14中的4台交换机，每台交换机都有端口位于VLAN 2中，哪是不是位于4台交换机上VLAN 2中的端口就构成了一个环路？是不是VLAN 2中的一个终端发送一个数据信号，这个数据信号就在这四台交换机中永不停息的传输下去，因为它们构成了一个环路？

其实不然，因为在Cisco交换机上默认是运行了生成树协议，生成树协议的运行目的就是要阻止交换机物理上的环路导致最终数据传输上的环路。它会把构成物理环路上的某个端口变成Blocked状态，从而把物理上的环路切断。如下所示是在3750-A和3750-D上执行“show spanning-tree interface interface-type”命令的显示结果：

```
3750-A#show spanning-tree interface g1/0/1
VLAN                Role Sts Cost      Prio.Nbr     Type
-------------       ---------------    --------     -----
VLAN0002             Root FWD 4          128.25      P2p
 //在3750-A执行显示生成树命令的显示结果
3750-D#show spanning-tree interface g1/0/2
VLAN                 Role Sts Cost           Prio.Nbr   Type
```

```
-------------    ---------------    --------    -----
VLAN0002         Root BLK 4          128.25      P2p
 //在3750-D执行显示生成树命令的显示结果
```

从上面的输出结果，可以看出在3750-A上的端口g1/0/1的状态为“FWD”，它是Forward的缩写，也就是VLAN 2中的数据传输到该端口，它会把接收到的VLAN 2中的数据转发出去。而在3750-D上的端口g1/0/2的状态为“BLK”，它是Blocked的缩写，也就是VLAN 2中的数据传输到该端口，它会阻塞接收到的VLAN 2中的数据继续传输下去，目的就是阻止环路的生成。也就是说3750-D上端口g1/0/2的阻塞状态，阻止了4台交换机在VLAN 2中生成环路的可能性。这其实也就是生成树的根本作用。

通过上面例“3”中的实例，依次介绍了VTP协议、Trunk技术和生成树协议3个知识点。从中也可以看出它们之间是环环相扣，紧密结合在一起使用的。

4. 总结

(1)学习。从事技术工作，不断地学习是每个技术工作者所必不可少的要求。就像上面例“1”中的GVRP协议，它的原理其实很简单，如果设备齐全的话，实施起来也很简单，但这前提是你必须去学习了解这个协议，并最终掌握它。只有这样，当你面对问题需要解决它时，才不至于手忙脚乱。如果做不到持续不断学习的话，是很难在工作中走到其他技术者的前列。

尤其是现在各种新技术不断涌现，不学习肯定就要落伍。在刚开始面对云计算和虚拟化，可能谁都不清楚它们的概念和具体的应用，只有查看、学习各种资料和书籍，了解它的定义。并且有条件的话，多参与实践学习，这样才能彻底掌握它，要不然面对新技术总是一头雾水。活到老，学到老，这句话尤其适用从事技术的工作者。

(2)实践。从事网络维护工作，是万万不能少了各种各样的实践操作。我自己从开始参加CCNA的培训，到后期的CCIE的培训，几乎每一堂课都有实践操作，都有实验。甚至在CCIE的培训中，绝大部分的时间和精力放在“CCIE集训营”、“CCIE LAB实验室”等这些实实在在的做实验上。这是因为我们学到的

每一个知识点，最终都要在实践中验证，通过做实验来说明它是正确的还是错误的。

包括平时在书本上或网络上看到一些知识点，可能在原理上都能明白，知道它们运行的机制和过程。但即使是这样，也只有通过把这些知识点涉及到的一些命令在交换机、路由器等设备上操作一遍，看看它们到底符合不符合书上所讲的结果。这样心底才能“踏实”地接受这个知识点，因为它经过了实践的检验！

所有从事网络工作者，一定要不断的给自己创造参与实践工作的机会。如果在工作中能接触到现成的网络设备更好，这样学习起来更方便。要是达不到这种条件的话，可以参加一些培训班，它们多多少少都能提供一些操作实验。实在不行，还可以使用一些模拟器，如Dynamips，它们所搭建起来的实验环境也很接近真实的网络环境。总之，一切网络知识，只有经过实践的检验，才能算它是正确的，也才能算自己真正掌握了它。

(3)总结。除非你有过目不忘的能力，否则，经常对所学到的知识点进行归纳总结是必不可少的。如果要把所有的知识点、操作命令都记在脑子里的话，这几乎是不可能的。因为现实中，制造网络设备的厂家会有很多种，它们可能为了实现同样一种功能，而使用了不同的操作命令。最典型的就是Cisco和H3C，前者的显示命令用是“show”，后面再加上各种参数来查看交换机或路由器的各种配置，而后者却是用“display”。另外，在这两个厂家设备上显示端口基本信息的命令上，前者是“show interface brief”，而后者是“display brief interface”，最后两个单词顺序还是相反的。这些知识点如果不进行提前总结记忆的话，到了要使用的时候才去熟悉和记忆，就会严重影响工作的效率。

另外，就像本篇文章所写的东西，其实也是一种总结。把相似的协议、相关的技术放到一起进行比较和分析。再把和协议相关的命令都罗列出来进行对比，加上一些相关的实例。这样以后在工作中，若再想了解、查看和使用这方面的协议和技术时，就只需打开这些文章，所有的相关知识就都一目了然，不用再去查各种各样的资料，或在网上搜来搜去的。这其实就是总结提高了工作效率。

2.4 运维实例：用MAC地址定位目标主机

网络结构图如图2-15所示。为了确保重要设备的稳定性和冗余性，核心层交换机使用两台Cisco4507，通过Trunk线连接。在两台核心交换机上连接有单位重要的服务器，如视频服务器、FTP、WEB和邮件服务器等。每台服务器都有两根网线分别连接到4507A和4507B上，以保证服务器和核心交换机之间传输数据的稳定性。单位IP地址的部署，使用的是C类私有192网段的地址。所有的服务器都位于VLAN 11～VLAN 20中，对应的网络号是192.168.11.0～192.168.20.0，如视频服务器的IP地址为192.168.11.8，子网掩码为255.255.255.0，默认网关为192.168.11.254。服务器的IP地址、默认网关和DNS都是静态配置的。

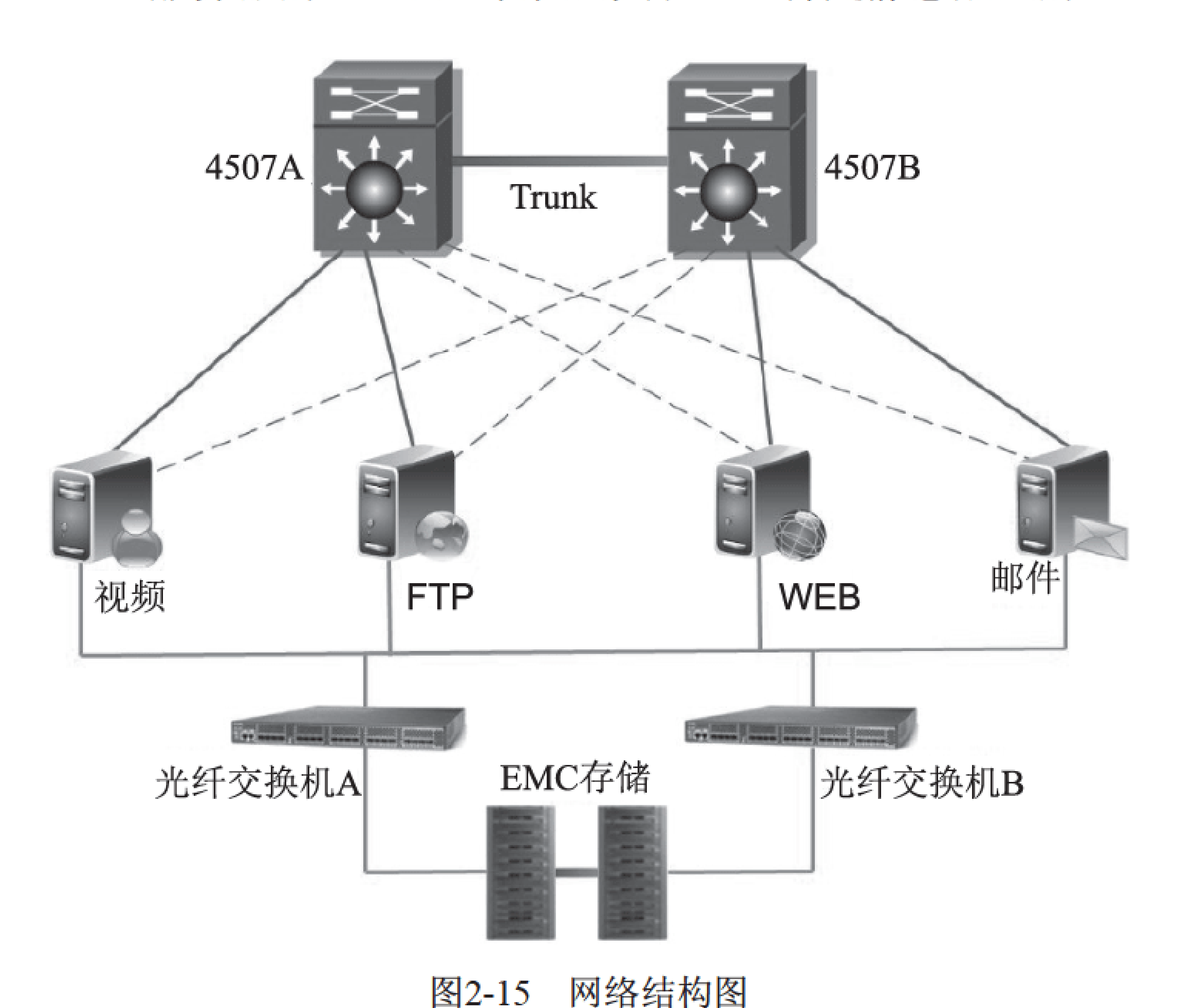


图2-15　网络结构图

因为服务器上数据的重要性，需要对数据进行存储、备份，所以每台服务器都使用HBA卡，再通过光纤连接到SAN网络中的光纤交换机上，再通过光纤交换机连接到EMC的存储、备份设备上。

1. 服务器应用系统升级引起的问题

因为业务扩充和应用系统升级的要求，需对视频服务器上的操作系统及应用软件进行重新安装。但在对视频服务器上的系统进行备份和规整时发现，服务器上有两块网卡都在使用。在视频服务器的操作系统Win 2003中的“命令行”中执行ipconfig /all命令，此命令能够显示当前系统的TCP/IP配置的设置值，并能用来检验人工配置的TCP/IP设置是否正确。执行命令后显示的结果如下所示：

```
C:\ >ipconfig  /all
Ethernet adapter 本地连接 1:
Description..........: Intel(R)PRO/1000 MT Network Connection
Physical Address..........: 00-13-72-42-24-50
IP Address..........: 10.1.1.12
Subnet Mask..........: 255.255.255.0
Ethernet adapter 本地连接 2:
Description..........: Intel(R)PRO/1000 MT Network Connection #2
Physical Address..........: 00-13-72-33-21-6F
IP Address..........: 192.168.11.8
Subnet Mask..........: 255.255.255.0
Default Gateway..........: 192.168.11.254
```

上面的输出结果中，其中192.168.11.8的IP地址，是视频服务器连接到单位办公网中所使用的地址。因为办公网中所有的PC、服务器及网络交换、路由设备都使用的是192网段的地址。

但是上面的显示中，还有另外一个10.1.1.12的IP地址，这个地址不是单位办公网中所使用的地址。但这个地址却是个活动地址，也就是在正常使用通过视频

服务器上的流量监控软件，能够看到10.1.1.12的网卡上有数据流量通过。那它是哪儿的地址？它是连接到什么设备上的？它是连接到什么网络中的？因为在机房视频服务器的日常工作记录本上，也没有和IP地址10.1.1.12相关的记录。但是要对视频服务器的应用系统进行升级，还必须弄明白服务器上所有IP地址的功能和用途。所以只能通过其他的方法查询10.1.1.12的功用了。

2. 解决问题的步骤

(1)既然知道视频服务器上有两个活动的IP地址192.168.11.8和10.1.1.12，那在服务器的ARP表中，也肯定有192.168.11.0/24和10.1.1.0/24这两个网段中的IP地址和MAC地址的对应项。所以在服务器的“命令行”中，执行“arp -a”命令。此命令是通过询问协议数据，显示当前的ARP表项。如果指定了特定的IP地址，则只显示指定计算机IP地址和物理地址的对应项。如果不止一个网络接口使用ARP，则显示每个ARP 表项。显示的结果如下所示：

```
C:\ >arp -a
Interface: 10.1.1.12 --- 0x10003
  Internet Address      Physical Address      Type
  10.1.1.2              00-60-16-0a-b5-a3     dynamic
Interface: 192.168.11.8 --- 0x10004
  Internet Address      Physical Address      Type
  192.168.11.4          04-1a-72-6a-4e-f2     dynamic
  192.168.11.254        01-80-0c-b7-a1-45     dynamic
```

由上面显示结果可以看出，192.168.11.0网段中的IP地址和MAC地址的对应项都是正常的，这些地址都是单位的办公网中正在使用的地址。

但是显示结果中的“10.1.1.2　00-60-16-0a-b5-a3　dynamic”项，是在单位办公网中没有使用的地址。不过配置10.1.1.2地址的设备，肯定是和视频服务器的10.1.1.12/24的网卡相连接的。

为了证实10.1.1.2的IP地址是活动的，就在视频服务器的“命令行”中执行了ping 10.1.1.2的命令，得到如下的显示：

```
C:\Users\Administrator>ping  10.1.1.2
正在 Ping 10.1.1.2 具有 32 字节的数据:
来自 10.1.1.2 的回复: 字节=32 时间=1ms TTL=255
来自 10.1.1.2 的回复: 字节=32 时间=1ms TTL=255
来自 10.1.1.2 的回复: 字节=32 时间=1ms TTL=255
来自 10.1.1.2 的回复: 字节=32 时间=1ms TTL=255
10.1.1.2 的 Ping 统计信息:
数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
最短 = 1ms，最长 = 1ms，平均 = 1ms
```

从上面的显示可以看出，10.1.1.2的IP地址也是处于活动状态的。

(2)现在已经知道和视频服务器IP地址为10.1.1.12的网卡相连的设备的IP地址和MAC地址。因为从10.1.1.12网卡连接出来的网线是通过机房的地下布线的。也就是说沿着视频服务器网卡后面的网线找各个连接点是非常困难的，因为所有的网线都在地板下，而地板上还放着服务器的机柜。

所以现在已经知道了10.1.1.2的IP地址和MAC地址，那能否在办公网中找到和这两个地址相关的信息，也就是在4507交换机的ARP表和CAM表中进行查找。

因为在三层交换机中都保存有这两张表，可以通过“show arp”命令查找连接到三层设备的客户端或服务器的IP地址和其MAC地址的对照表。通过“show mac address-table”查找连接到二层设备的客户端或服务器的MAC地址和其连接到二层设备接口的对照表。也就说只要知道其中的某一个就可以知道另一个的值。也可以说三层设备维护的是ARP表，二层设备维护的是CAM表。因为三层

交换机同时具备三层、二层功能，所以这两张表它都进行维护。

但是在4507中执行“Cisco4507#show arp | include 10.1.1.2”和“Cisco4507#sh mac address-table dynamic | include 0060.160a.b5a3”两条命令后，并没有任何结果显示，如下所示：

```
Cisco4507#sh arp | include 10.1.1.2
Cisco4507#
Cisco4507#sh mac address-table dynamic | include
0060.160a.b5a3
Cisco4507#
```

从上面的输出中可以看出，在4507的ARP表和CAM表中并没有包含“10.1.1.2”和“0060.1601.b5a3”的表项。若是在这两个表中包含某一参数的话，一般会得到和下面格式一致的输出结果：

```
Cisco4507#sh arp | include 192.168.2.1
Protocol  Address Age (min) Hardware Addr Type  Interface
Internet  192.168.2.14  0 131d.920d.1a32  ARPA  VLAN 2
Internet  192.168.2.1  0  1613.7868.4a9d  ARPA  VLAN 2
Cisco4507#sh mac address-table dynamic | include 1223.8916.1227
VLAN  mac address  type  protocols  port
200  1223.8916.1227  dynamic ip  GigabitEthernet3/1
```

同时在4507上执行命令“Cisco4507#ping 10.1.1.2”，得到如下输出结果：

```
C:\Users\Administrator>ping 10.1.1.2
正在 Ping 10.1.1.2 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。
10.1.1.2 的Ping统计信息:
数据包：已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)，
```

从上面的输出结果可以看出，在单位的办公网中，并没有IP地址是10.1.1.2的这个设备。

(3)因为MAC地址具有唯一性，并和物理设备绑定在一起，而IP地址并不具备这两个特性，所以，现在只能通过MAC地址进行查找IP地址10.1.1.2具体是什么设备，并确定它的物理位置。

MAC地址是识别局域网节点的标识，是烧录在网卡(Network Interface Card，NIC)里，共48比特长，由12个十六进制的数字组成，其中0～23位为组织唯一标识符，24～47位是由厂家自己分配。网卡的物理地址通常是由网卡生产厂家烧入网卡的可擦写可编程只读存储器中，它存储的是传输数据时真正赖以标识发出数据的电脑和接收数据的主机的地址。MAC地址的前6个十六进制的数字是由IEEE进行分配的。通过IEEE的网站，就能查询到MAC地址前6个十六进制的数字和其使用公司名称的对应关系。

因为现在知道了IP地址10.1.1.2和其对应的MAC地址00-60-16-0a-b5-a3。所以在一台能访问互联网的电脑的浏览器地址栏中输入，通过MAC地址查询网卡生产厂商的IEEE的网址“http://standards.ieee.org/develop/regauth/oui/public.html”，打开后，在页面中输入地址“00-60-16-0a-b5-a3”的前六位，然后单击按钮“Search！”，如图2-16所示。

Search the Public OUI/'company_id' Listing

Search for: 00-60-16 Search! clear field

Download a copy of the OUI Public Listing (Updated daily)

图2-16　通过MAC地址查询公司名称图示

单击查询后，会得到如下的显示结果：

```
    Here are the results of your search through the public
section of the IEEE Standards OUI database report for 00-60-16:

    ------------------------------------------------------------

    00-60-16    (hex)              CLARIION

    006016     (base 16)           CLARIION

                                   COSLIN DRIVE

                                   Mail Stop C25

                                   SOUTHBORO MA 01772

                                   UNITED STATES
```

由上面的输出结果可以看出，IP地址是10.1.1.2的设备类型是“CLARIION”，它是EMC存储产品中的一个系列产品，属于中端存储产品，所以，现在就能确定10.1.1.12和10.1.1.2两个IP地址都是应用在存储设备上，也就能确定10.1.1.2的具体位置在EMC的存储设备上。

(4)确定IP地址的具体位置。打开EMC的机柜后，发现在其中有一个五端口的交换机，它是EMC厂家自带的，五端口交换机上的接口全是电口，上面都接有网线。如图2-17所示，是视频服务器连接EMC自带交换机的示意图。

为了确认视频服务器，10.1.1.12网卡上的网线是不是接到EMC机柜中的五端口交换机上，我们把10.1.1.12网卡上的网线拔掉，结果五端口交换机上一个端口的指示灯就灭了，把网线插上后，交换机上那个端口的指示灯又亮了。

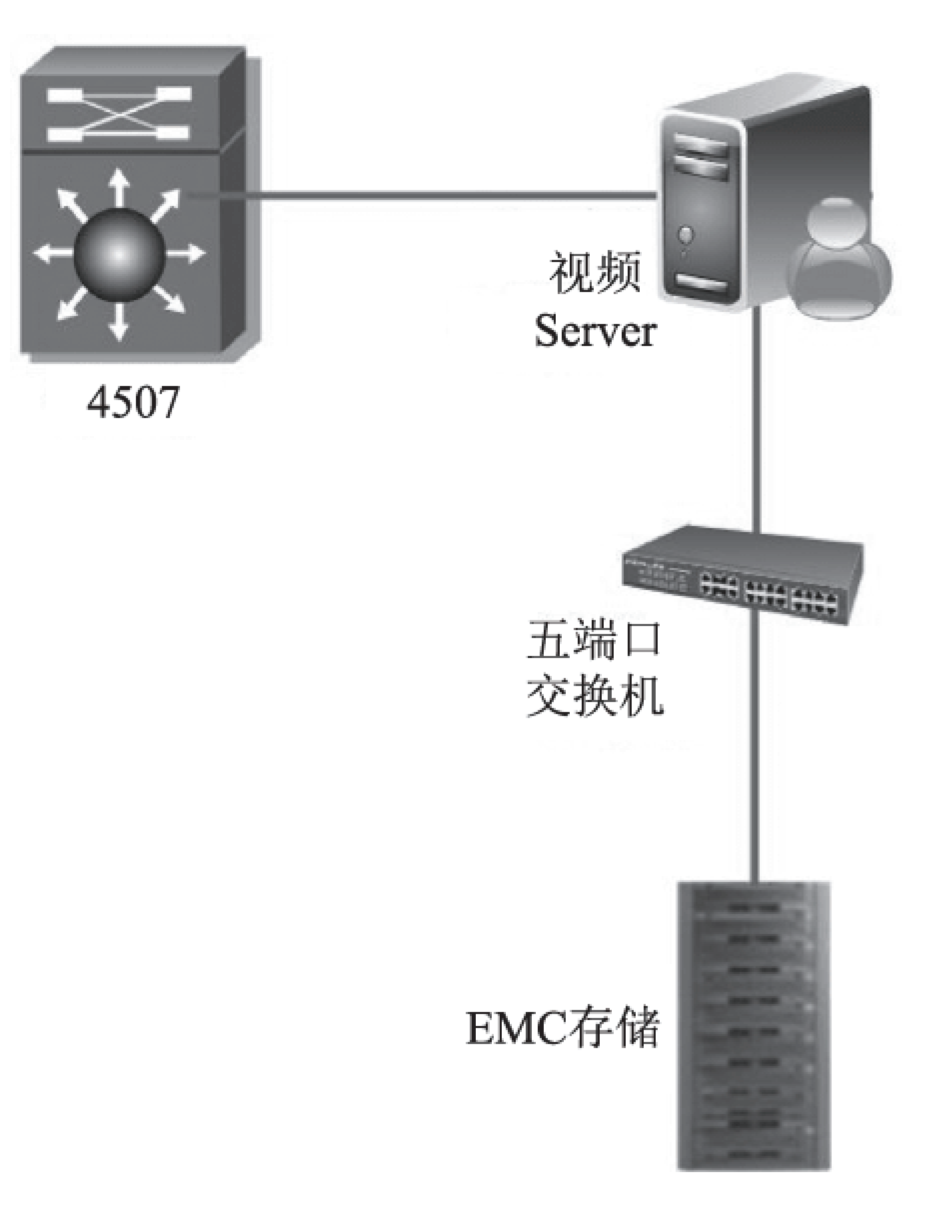


图2-17　视频服务器连接EMC自带交换机图示

所以，现在就能确定视频服务器上IP地址是10.1.1.12的网卡是通过EMC的五端口交换机连接到EMC的存储设备上，10.1.1.2就是EMC存储设备上电口的IP地址。10网段中的地址都是用来在视频服务器上对EMC的存储设备进行远程操作控制所使用的。

明白了IP地址所使用的具体位置和其功能后，就可以放心的对视频服务器进行重装系统和应用软件的升级了。如图2-18所示，是EMC机柜图。



图2-18　EMC机柜图示

3. 总结

(1)由以上解决问题的步骤，可以看出，在视频服务器上共连接有3根网络数据线。第1根是双绞线，通过IP地址是192.168.11.8的网卡连接到核心交换机4507上。这根网线的主要作用是让单位办公网络中的客户端能通过4507核心交换机访问到视频服务器上的资源。第2根是光纤，通过视频服务器的HBA卡，连接到存储区域网络(Storage Area Network， SAN)中的光纤交换机上，再通过光纤交换机连接到EMC的存储设备上。这根光纤的主要作用是对视频服务器上数据库中的数据进行存储、备份，通过光纤传输数据也能够大大提高数据传输的速率。第3根也是双绞线，通过IP地址是10.1.1.12的网卡连接到EMC自带的五端口交换机上，这根网线的主要作用是在视频服务器上通过WEB管理控制界面对EMC存储设备进行管理和配置。

(2)MAC地址具有全球唯一性，利用这种特性往往能给排查网络故障带来很大的便利性。因为MAC地址和设备是绑定在一起的，只要做好了MAC地址和具体设备对应关系的维护登记工作，那只要知道了MAC地址，就能找到MAC地址对应的设备在哪里。

而IP地址并不具有这种特性，IP地址更多的是一种逻辑上的地址，通常情况下IP地址和具体的设备并不是一一对应的，尤其是使用了DHCP和NAT技术后，IP地址和设备之间并没有什么关系。使用DHCP技术后，客户端和服务器获取到的IP地址都是动态和变化的，今天使用的是A地址，明天可能就使用的是B地址。而NAT技术的变化更大，如局域网中的用户使用NAT技术和互联网上的用户进行通信，互联网上的用户看到局域网中用户使用的IP地址，实际上并不是他的实际IP地址，所以这时要把IP地址与具体的设备或用户联系起来，是非常困难的。

使用IP地址的这种不确定性，在随着以后IPv6使用范围的不断推广，就会有很大的改观。因为IPv6地址数量的庞大，按保守方法估算，IPv6实际可分配的地址，在整个地球每平方米面积上可分配1000多个地址，号称能让“每颗沙子都拥有一个IP地址”。既然IPv6有这么多的地址，能保证每一个Internet上的终端使用的都是全球唯一IP地址，所以当IPv6地址在全球普及的时候，也就保证了每一个IPv6地址能与具体的设备和用户对应起来，这对网络安全和网络维护工作将带来很大便利。

(3)其实这次网络问题的排查，若是以前在维护和配置视频服务器时能够按照规定，对操作规程进行严格的登记和记录，这样在解决上面的问题时，只要看下记录本，所有的东西都一目了然了。也就大大节省了网络维护人员的时间和精力，提高了工作效率。看来注重点滴和基础工作，对网络维护、管理工作也是必不可少的。

2.5　运维实例：交换机虚拟接口应用

目前，三层交换机已在企业网络中普遍应用。在本质上三层交换机实际上就是具有路由功能的二层交换机。路由是属于第三层的功能，所以带有路由功能的交换机就被称为三层交换机。而在三层交换机中跨VLAN间路由，就要使用SVI(Switch Virtual Interface，交换机虚拟接口)，SVI的作用就是用于各个VLAN间转发数据的接口。与传统的路由器相比，它可以实现高速的路由。

下面就通过3则实例，每一则实例中都包括一副拓扑图。3幅拓扑图所要实现的功能是一样的，都是为了让位于不同VLAN中的PC1和PC2之间能互相通信。但是3幅拓扑图中设备的配置命令是不一样的。通过3种不同的配置命令，而实现相同的功能，从而达到深刻理解SVI的功能和原理。

1. 实例一

如图2-19所示，图中左边部分共使用了3台交换机和两台PC。PC1和PC2的IP地址分别配置为172.16.2.1/24和172.16.3.1/24，其中在3台交换机上都要创建二层的VLAN 2和VLAN 3，并且把PC1划入到VLAN 2，PC2划入到VLAN 3。在Cisco2960上，把F0/2和F0/12划入到VLAN 2，把F0/3和F0/13划入到VLAN 3。在Cisco3750上，把G1/0/2划入到VLAN 2，把G1/0/3划入到VLAN 3。这样配置后就能保证PC1、Cisco2960的F0/2、F0/12 和Cisco3750的G1/0/2都位于VLAN 2中，同样PC2、Cisco2960的F0/3、F0/13 和Cisco3750的G1/0/3就都位于VLAN 3中。

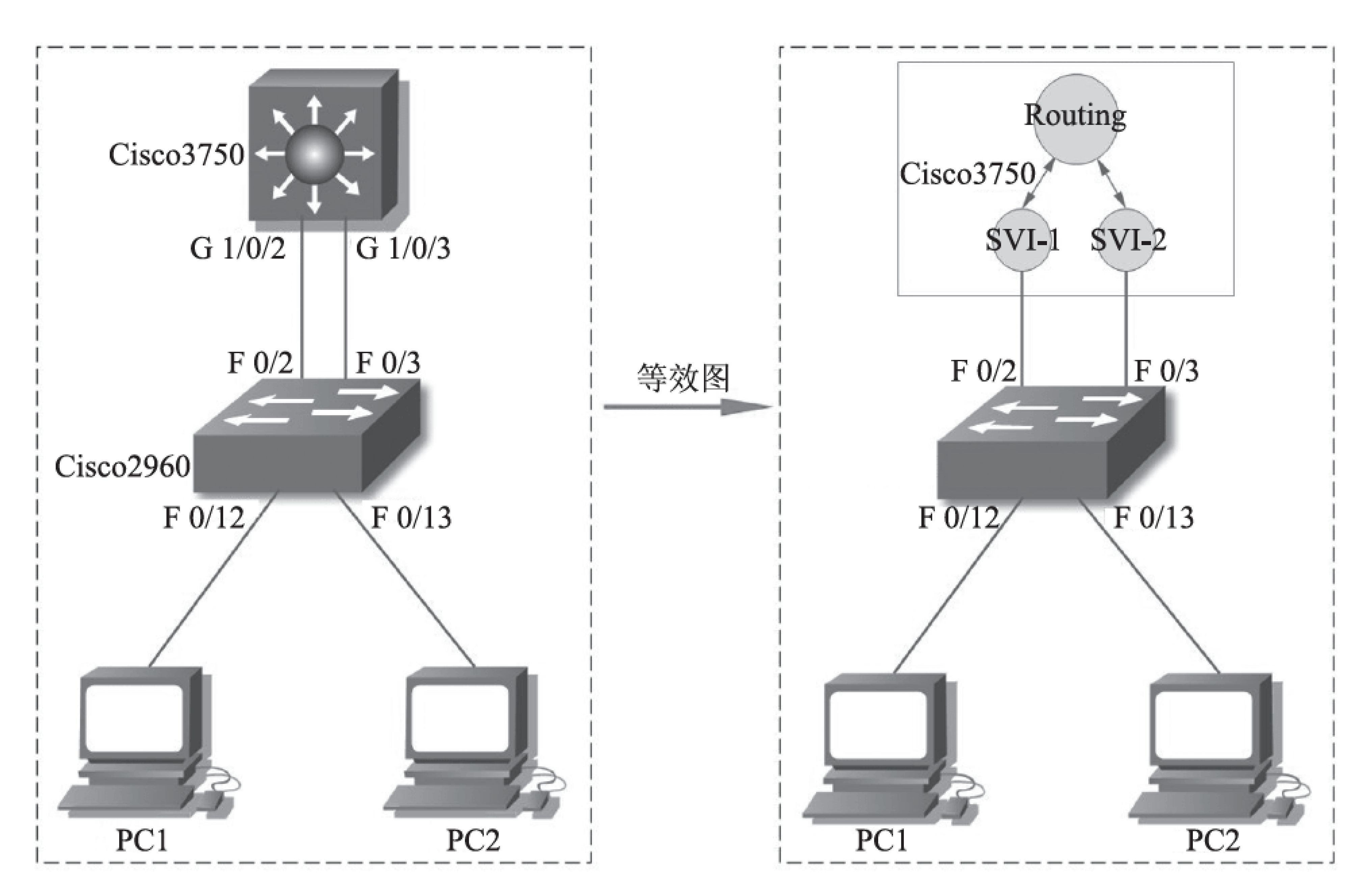


图2-19　利用SVI接口实现VLAN间路由

在同一个VLAN中的设备相互间可以直接通信，但是若要在不同的VLAN间通信，一般的情况下就要借助路由设备。不过，若是有三层交换机，就可以利用三层交换机的SVI接口，实现不同VLAN之间的通信。这里就应用了Cisco3750上的SVI接口，它们的作用就是充当二层VLAN 2和VLAN 3 对外收发数据的三层接口。图2-19的右边部分，相当于左边部分的原理图，二者是等效的。通过右边部分的图示，能够更深刻地理解SVI的运行原理。下面是在Cisco3750上创建SVI接口的配置命令：

```
Cisco3750(config)#int vlan 2
Cisco3750(config-if)#ip address 172.16.2.254 255.255.255.0
Cisco3750(config-if)#no shutdown
Cisco3750(config-if)#int VLAN 3
Cisco3750(config-if)#ip address 172.16.3.254 255.255.255.0
Cisco3750(config-if)#no shutdown
```

创建完SVI接口后，172.16.2.254和172.16.3.254就分别作为二层VLAN 2和VLAN 3的默认网关。其中在Cisco3750上还有很重要的一条命令“Cisco3750(config)#ip routing”必须进行配置，它的作用是启用3750的路由功能，否则三层交换机只能使用其二层交换功能，这样位于不同子网的PC1和PC2相互间肯定就不能通信了。在Cisco3750上配置完成后，PC1就能ping通PC2了，如图2-20所示，是在PC1上所做的ping测试。

```
C:\Users\Administrator>ping 172.16.3.1

正在 Ping 172.16.3.1 具有 32 字节的数据:
来自 172.16.3.1 的回复: 字节=32 时间=4ms TTL=255
来自 172.16.3.1 的回复: 字节=32 时间=1ms TTL=255
来自 172.16.3.1 的回复: 字节=32 时间=3ms TTL=255
来自 172.16.3.1 的回复: 字节=32 时间=2ms TTL=255

172.16.3.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 4ms, 平均 = 2ms
```

图2-20　PC1能ping通PC2

SVI接口是在三层交换机的全局配置模式下，使用命令“interface VLAN”，后面键入具体的VLAN ID时创建的。当需要路由虚拟局域网之间的数据，就要为相应的虚拟局域网配置相应的SVI接口，通常也把这种接口称为逻辑三层接口，也就是三层接口。可以用“no interface VLAN VLAN_id”全局配置命令来删除对应的SVI接口。只是不能删除VLAN 1的SVI接口，因为VLAN 1接口是默认已创建的，用于管理远程交换机。SVI是联系二层VLAN的IP接口，一个SVI只能和一个VLAN相联系。

2. 实例二

实例二与实例一不同的地方，就是使用了路由器Cisco2811代替Cisco3750，这种架构就是通常情况下借助路由器实现不同VLAN间的通信。其中在Cisco2960上和实例一中有变化的地方，就是把F0/1配置成了Trunk口，命令为“Cisco2960(config-if)#switchport mode trunk”，这样配置后，就允许VLAN 2和VLAN 3的数据通过F0/1到达路由器Cisco2811的F0/0接口。另外，在Cisco2811的F0/0上也要配置两个子接口，命令如下：

```
Cisco2811(config)#int fa0/0
Cisco2811(config-if)#no ip address
Cisco2811(config)#int fa0/0.2
Cisco2811(config-subif)#encapsulation dot1q 2
Cisco2811(config-subif)#ip address 172.16.2.254 255.255.255.0
Cisco2811(config)#int fa0/0.3
Cisco2811(config-subif)#encapsulation dot1q 3
Cisco2811(config-subif)#ip address 172.16.3.254 255.255.255.0
```

命令配置完成后，同样可以实现PC1和PC2之间的通信。和实例一相比，只是在Cisco2960上，用Trunk口F0/1代替了实例一中的F0/2和F0/3。在Cisco2811上用F0/0.2代替了Cisco3750上的SVI-1，也就是用命令“Cisco3750(config)#int VLAN 2”创建的三层虚拟接口。用F0/0.3代替了3750上的SVI-2接口。Cisco2811通过在F0/0.2和F0/0.3之间路由数据，最终实现了二层VLAN 2和VLAN 3之间的通信，如图2-21所示。

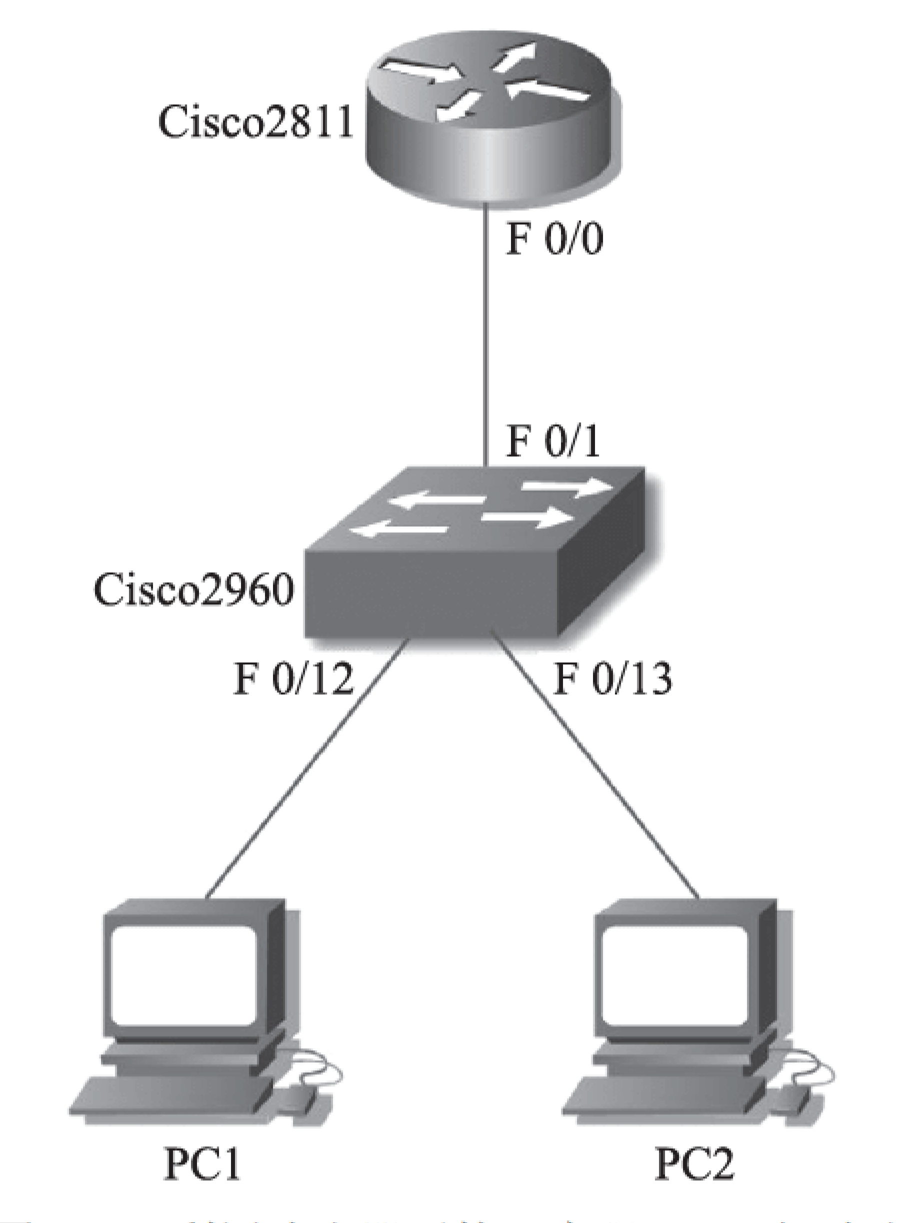


图2-21　利用路由器子接口实现VLAN间路由

3. 实例三

实例三与实例一中使用的设备完全一样，只是配置命令有所区别。G1/0/2和G1/0/3不再是二层接口，它们已具有三层功能，并配置了IP地址。这两个端口的作用就相当于实例一中的SVI-1和SVI-2的作用，也和实例二中的Cisco2811上的F0/0.2、F0/0.3作用是一样的，都是为转发二层VLAN 2和VLAN 3中的数据提供了一个三层的出入接口，如图2-22所示。实例三中与实例一中的Cisco2960的配置完全一样，变化的只是Cisco3750上的配置，如下所示：

```
Cisco3750(config)#int g1/0/2
Cisco3750(config-if)#no switchport
Cisco3750(config-if)#ip address 172.16.2.254 255.255.255.0
Cisco3750(config-if)#int g1/0/3
Cisco3750(config-if)#no switchport
Cisco3750(config-if)#ip address 172.16.3.254 255.255.255.0
```

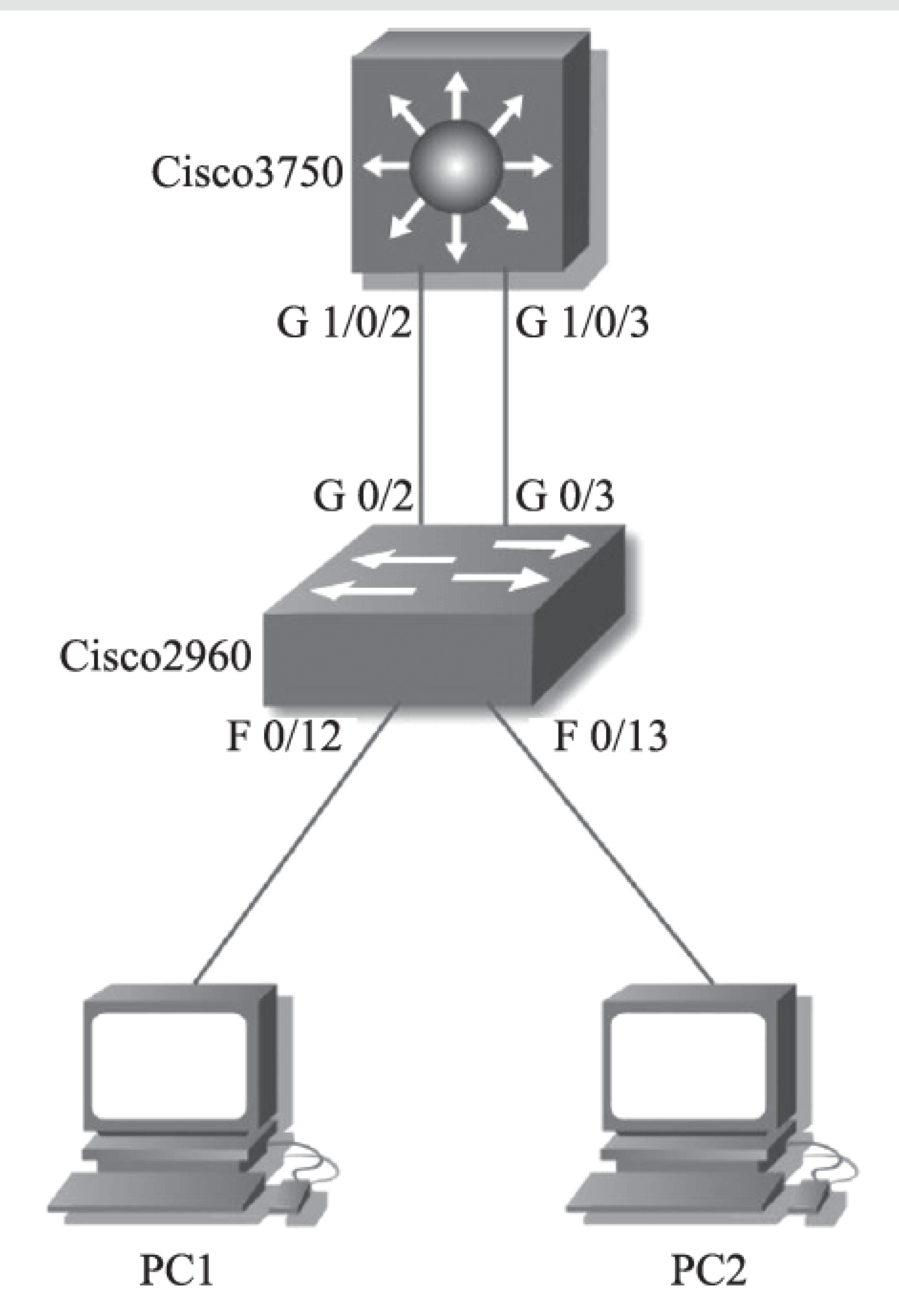


图2-22 利用交换机三层端口实现VLAN间路由

注意：必须在两个接口上配置no switchport命令，否则两个端口只能作为二层端口使用，也就不能配置IP地址。同样，在Cisco3750上也必须配置“Cisco3750(config)#ip routing”命令。在这种通信模式中，三层交换机3750实际上就相当于一台路由器，使用命令show ip route，可以查看路由表中的内容，如下所示：

```
Cisco3750#show ip route
Gateway of last resort is not set
 172.16.0.0/24 is subnetted, 2 subnets
C 172.16.3.0 is directly connected, GigabitEthernet1/0/3
C 172.16.2.0 is directly connected, GigabitEthernet1/0/2
```

4. 总结

(1)通过上面在功能上相互等效的3个实例，可以看出SVI的本质，就是内置在三层交换机中的一个三层接口，和一般的三层接口在功能上是完全一样的。它们可以作为交换机的管理接口，管理员可以远程管理该交换机。也可以作为网关接口，用于三层交换机跨VLAN间路由。

(2)目前，使用路由器在VLAN之间路由数据的网路架构越来越少。随着VLAN之间流量的不断增加，因为路由器是基于软件处理的，即使它能以线速度接收到数据包，也无法在不限速的条件下把数据包都转发出去，因此路由器在路由不同VLAN间的数据时，经常会成为整个网络的瓶颈。而三层交换机使用专用硬件芯片处理数据帧的交换操作，利用SVI接口，快速实现数据帧的交换，所以它已在中型和大型的企业网络中得到了普遍应用。

2.6　运维实例：网络中主机间5种简单通信模式

目前，现实中的计算机网络错综复杂，令人眼花缭乱。但从本质上来说，这些网络无非是实现终端间的互相通信，终端上都配置有IP地址和MAC地址。下面就以5种通信模式，对目前经常使用的计算机网络进行归纳总结，以便网络技术人员再遇到复杂的网络时，能很快明白其运行的机制和原理。

1. 通过网线直接互连两台主机间的通信模式

这种通信方式，大部分人都实验过，也比较简单。PC_A和PC_B的IP地址分别配置为10.1.1.2/24和10.1.1.3/24，两台主机在同一个子网中，如图2-23所示。相互通信前，主机利用ARP协议，知道了对方的MAC地址，才能进行二层通信。需要注意的是，连接两台电脑的网线是交叉线，一端是T568A，一端是T568B。不能使用直通线，否则，两台电脑无法通信。



图2-23　两台主机通过网线通信

2. 同一VLAN中主机间的通信

这种通信模式中使用了一台Cisco3750三层交换机，但通信过程中只使用了它的二层功能，没有启用三层路由功能。这种模式虽然简单，但使用却非常普遍，基本上在所有的计算机网络中都会使用到。PC_A和PC_B的IP地址分别配置为10.1.1.2/24和10.1.1.3/24，如图2-24所示。在Cisco3750上首先要创建VLAN 2，命令如下：

```
Cisco3750#VLAN database
Cisco3750(VLAN)#VLAN 2
```

```
VLAN 2 added:
Name: VLAN0002
```

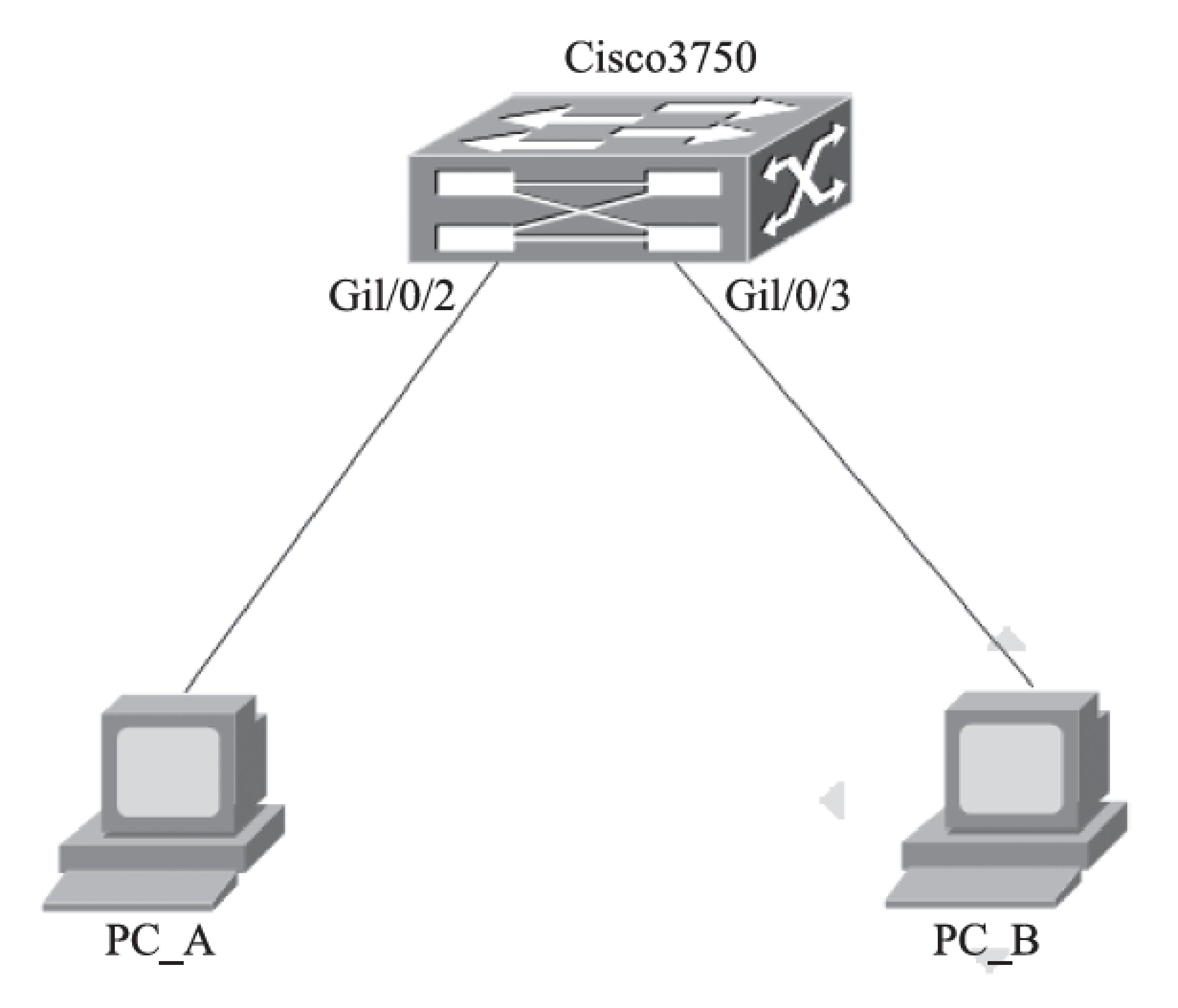


图2-24 两台主机在同一VLAN中通信

最终Cisco3750的配置如下所示：

```
hostname Cisco3750
!
interface GigabitEthernet1/0/2
 switchport access VLAN 2
 switchport mode access
!
interface GigabitEthernet1/0/3
 switchport access VLAN 2
 switchport mode access
```

因为两台主机都位于VLAN 2中，它们也就在同一个子网10.1.1.0/24中。在这种模式中，PC_A和PC_B的通信是在二层进行的，也就是通过MAC地址通信。

3. 不同VLAN中的主机通过SVI接口通信

Cisco三层交换机SVI(Switch Virtual Interface，交换机虚拟接口)是在三层交换机的全局配置模式下使用“interface VLAN”命令，后面键入具体的VLAN ID时创建的。当需要路由虚拟局域网之间的流量，就要为相应的虚拟局域网配置相应的SVI接口，通常也把这种接口称为逻辑三层接口，也就是三层接口。可以用“no interface VLAN VLAN_id”全局配置命令来删除对应的SVI接口，只是不能删除VLAN 1的SVI接口，因为VLAN 1接口是默认已创建的，用于管理远程交换机。SVI是联系二层VLAN的IP接口，一个SVI只能和一个VLAN相联系。

在这种通信模式中，PC_A和PC_B的IP地址分别配置为10.2.2.2/24和10.3.3.3/24，并且分别位于3750的VLAN 2和VLAN 3中，网络结构图和图2-24一样，只是主机的IP地址和3750的配置有所变化。同时在3750上也要创建VLAN 2和VLAN 3的SVI接口，命令如下：

```
Cisco3750(config)#int VLAN 2
Cisco3750(config-if)#ip address 10.2.2.254 255.255.255.0
Cisco3750(config-if)#no shutdown
Cisco3750(config-if)#int VLAN 3
Cisco3750(config-if)#ip address 10.3.3.254 255.255.255.0
Cisco3750(config-if)#no shutdown
```

配置IP地址后，10.2.2.254和10.3.3.254就分别作为VLAN 2和VLAN 3的默认网关。3750上最终的配置如下所示：

```
hostname Cisco3750
!
```

```
ip routing
!
interface GigabitEthernet1/0/2
 switchport access VLAN 2
 switchport mode access
!
interface GigabitEthernet1/0/3
 switchport access VLAN 3
 switchport mode access
!
interface VLAN 2
 ip address 10.2.2.254 255.255.255.0
!
interface VLAN 3
 ip address 10.3.3.254 255.255.255.0
```

其中“ip routing”命令是启用3750的路由功能，否则三层交换机只能使用其二层交换功能，这样位于不同子网的PC_A和PC_B相互间就不能通信了。在3750上配置完成后，PC_A就能ping通PC_B，如图2-25所示是在PC_A上所做的ping测试。

```
C:\Users\Administrator>ping 10.3.3.3

正在 Ping 10.3.3.3 具有 32 字节的数据:
来自 10.3.3.3 的回复: 字节=32 时间<1ms TTL=127
来自 10.3.3.3 的回复: 字节=32 时间<1ms TTL=127
来自 10.3.3.3 的回复: 字节=32 时间<1ms TTL=127
来自 10.3.3.3 的回复: 字节=32 时间<1ms TTL=127

10.3.3.3 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms，最长 = 0ms，平均 = 0ms
```

图2-25　在PC_A上ping主机PC_B

4. 通过交换机三层端口实现主机间通信

在这种通信模式中，PC_A和PC_B的IP地址还是10.2.2.2/24和10.3.3.3/24，网络结构图和图2-24一样，变化的是3750上的配置，其中要关闭G1/0/2和G1/0/3两个端口的交换功能，关闭交换功能的同时也就启用了这两个端口的路由功能。配置的命令如下所示：

```
Cisco3750(config)#int g1/0/2
Cisco3750(config-if)#no switchport   //关闭端口的交换功能
Cisco3750(config-if)#ip address 10.2.2.254 255.255.255.0
Cisco3750(config-if)#no shutdown
Cisco3750(config-if)#int g1/0/3
Cisco3750(config-if)#no switchport  //关闭端口的交换功能
Cisco3750(config-if)#ip address 10.3.3.254 255.255.255.0
Cisco3750(config-if)#no shutdown
```

注意，必须配置no switchport命令，否则下面的IP地址命令是无法配置的。最终3750上的配置如下所示：

```
hostname Cisco3750
!
ip routing
!
interface GigabitEthernet1/0/2
 no switchport
 ip address 10.2.2.254 255.255.255.0
```

```
!
interface GigabitEthernet1/0/3
 no switchport
 ip address 10.3.3.254 255.255.255.0
```

这种通信模式中，三层交换机3750实际上就相当于一台路由器，使用命令“show ip route”就可以查看路由表中的内容，如下所示：

```
Cisco3750#show ip route
Gateway of last resort is not set
 10.0.0.0/24 is subnetted, 2 subnets
C  10.3.3.0 is directly connected, GigabitEthernet1/0/3
C  10.2.2.0 is directly connected, GigabitEthernet1/0/2
```

5. 通过SVI接口和三层口实现主机间通信

这种通信模式其实就是上面第2种和第3种两种通信模式的结合。把PC_A划到VLAN 2中，交换机G1/0/2端口配置为二层端口，并且把PC_A的默认网关指向VLAN 2的SVI接口地址10.2.2.254/24。PC_B连接的3750的端口G1/0/3还是三层口，其IP地址为10.3.3.254/24，如图2-26所示。

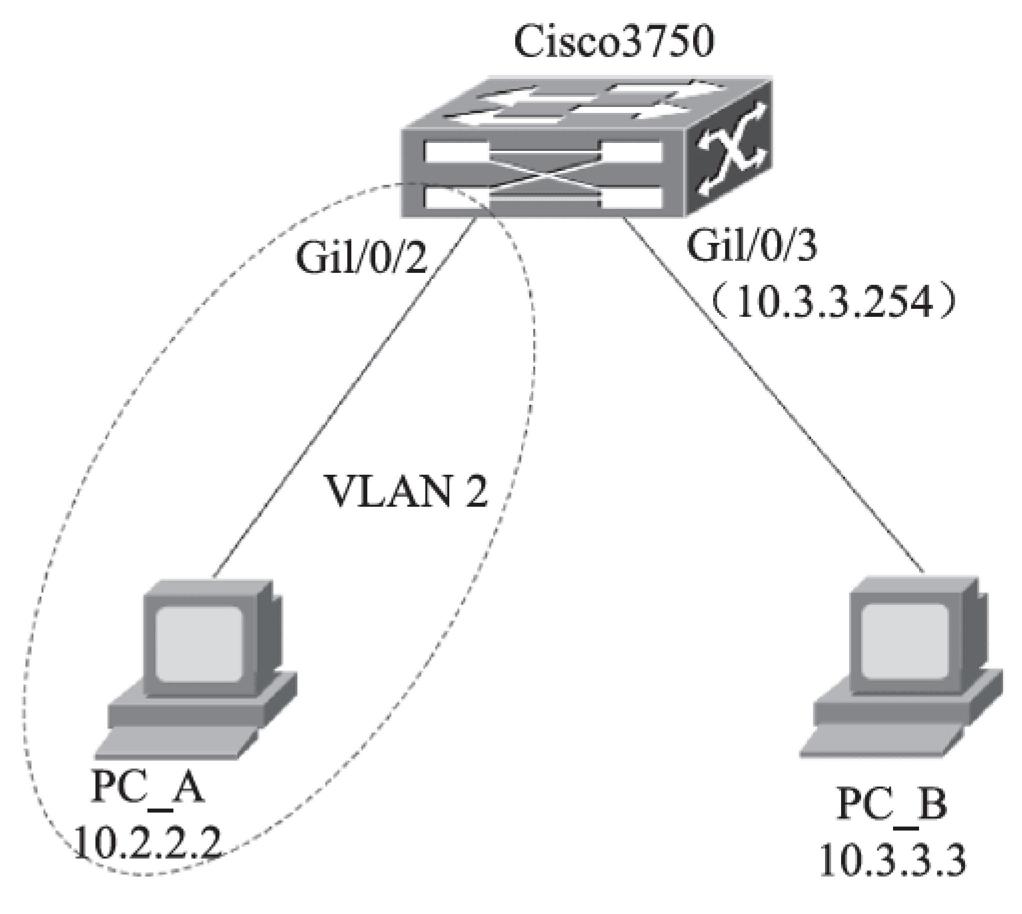


图2-26　通过SVI接口和三层口实现通信

最终3750上的配置如下所示：

```
hostname Cisco3750
!
ip routing
!
interface GigabitEthernet1/0/2
 switchport access VLAN 2
switchport mode access
!
interface GigabitEthernet1/0/3
 no switchport
 ip address 10.3.3.254 255.255.255.0
!
interface VLAN 2
 ip address 10.2.2.254 255.255.255.0
```

6. 总结

通过对照以上5种通信模式，首先，能看出三层交换机SVI接口的作用，它其实就相当于一个路由口。第2种通信模式中的interface VLAN 2接口和第4种通信模式中的G1/0/2接口的作用和运行原理是一样的，这在第5种通信模式中就得到了验证。其次，上面5种通信模式，后3种可以划为一类，它们都是使用IP地址通信，属于三层通信，而前两种通信模式中的数据传输使用的是MAC地址，属于二层通信。

第3章

网络运维技巧

从事网络运维工作，离不开大量的实践工作。若要运用从书本上学到的理论知识，去解决现实运维中碰到的实际问题，往往会有很大的偏差。一个高水平的网络运维工程师肯定是建立在大量实践工作基础之上的，而网络运维的技巧就是在这些大量的实际工作中慢慢总结和摸索出来的。

比如在一个小型企业中，所有的公司员工都要共同使用一套OA办公应用系统，理所当然，此系统安装在局域网中的一台服务器上最为妥当，OA服务器和员工的办公电脑就都位于同一个VLAN中，用户只需要在浏览器的地址栏中输入OA应用系统服务器的IP地址，例如209.12.56.78，就可访问OA系统了，但这时就会遇到一个问题，让用户记忆枯燥的IP地址，不但不易记，且易出错，那这时使用域名就是最好的解决办法，比如说可以用www.oa.com代替那烦人、难记的IP地址。但为一个局域网的用户分配和购买一个域名，就有些小题大做了。

这时配置、修改用户的Hosts文件就是最好的方式，只需在每位用户的Hosts中，添置项目“209.12.56.78 www.oa.com”即可。这时对网络运维人员来说，在每个用户的电脑上添加可能也很费事，网络运维工程师可以制作一个BAT的可执行文件，用QQ或其他即时通讯工具群发给所有用户，然后让用户在各自的电脑上执行此BAT文件即可。这样用户访问OA系统时，肯定都能记住此地址了。

这里再列举一个例子，作为网络运维师，测试网络的连通性那是常有的事，最常见的情形就是工程师拿着一个笔记本电脑，跑到东把一根网线的接头插入到笔记本的网口上，然后在键盘上砰、砰、砰……，敲入一连串的参数，过一会又跑到西，再重复刚才相同的动作，这就是一个外行人眼中一个网络运维人员最常见的情形。

但是工程师在做上面的事情时，重复率最高的一件事就是配置笔记本网卡的网络参数，每次都要重新配置网卡的IP地址、子网掩码和默认网关地址及DNS地址。看似简单的一件事，但若要多次重复的话，也是很费时费力的。提高生产效率，往往是在做多次重复性的低效率的事情后慢慢总结、归纳出来的。所以，解决上面的问题，最高效的办法就是使用BAT可执行文件，欲知解决办法的详细内容，请看官阅览本章3.2节内容。

3.1　运维实例：巧妙利用HOSTS文件替代DNS域名解析

网络结构图如图3-1所示。为了确保重要设备的稳定性和冗余性，核心层交换机使用两台Cisco6506-E，通过Trunk线连接。在分布层使用了多台Cisco3750-E交换机，图示为了简洁，只画出了两台。在核心交换机上连接有单位重要的服务器，如FTP、DHCP、E-MAIL服务器和DNS服务器等。单位IP地址的部署，使用的是C类私有192网段的地址。其中，FTP服务器的IP地址为192.168.2.8。Cisco6506-E和Cisco3750-E之间也是Trunk连接。

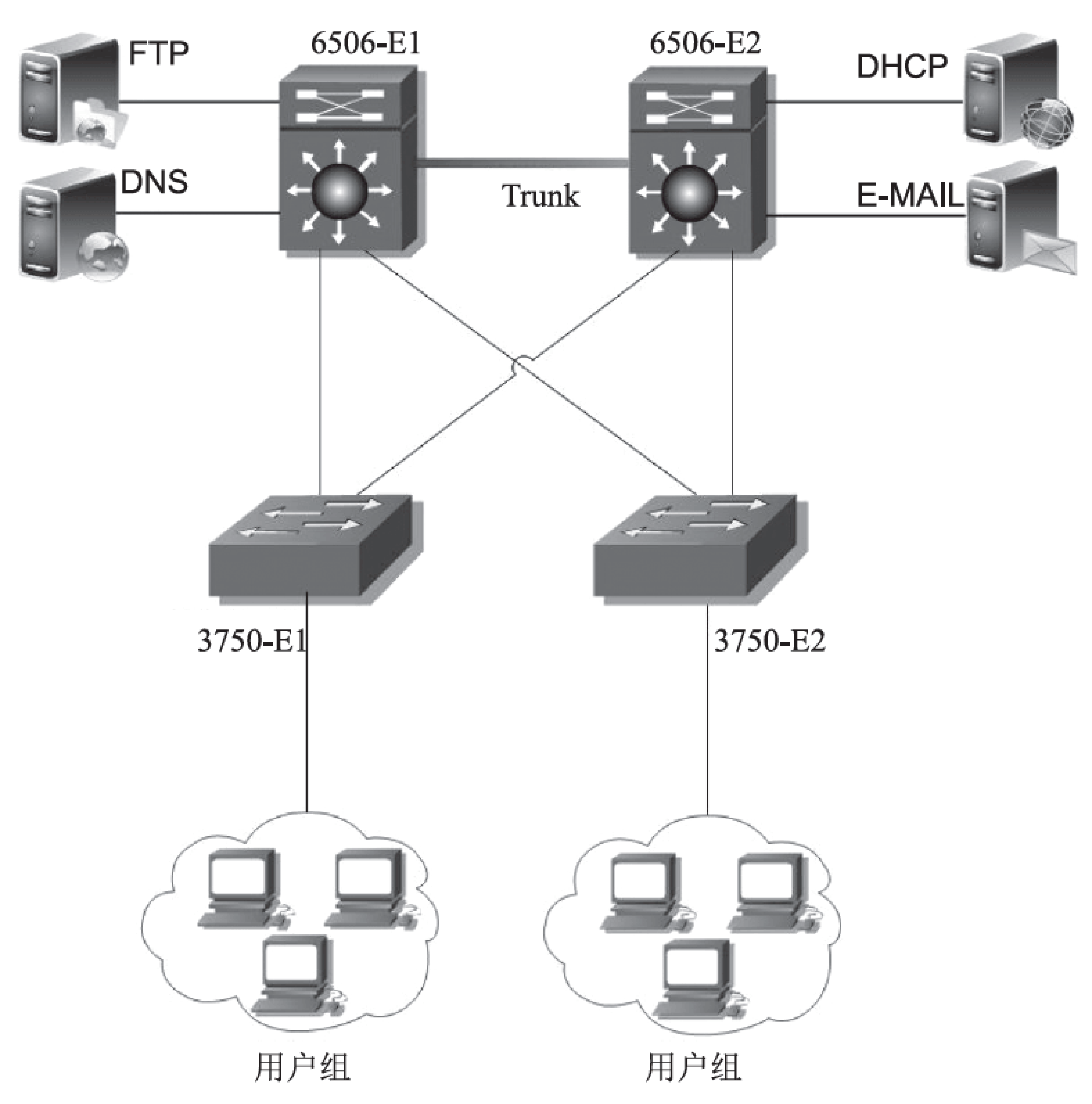


图3-1　网络结构图

公司根据部门性质的不同，把它们划入到不同的VLAN中。服务器都

位于VLAN 2～VLAN 10中，对应的网络号是192.168.2.0～192.168.10.0，如FTP服务器位于VLAN 2中。服务器的IP地址、默认网关和DNS都是静态配置的。VLAN 11～VLAN 200是属于各个部门使用，对应的网络号是192.168.11.0～192.168.200.0。VLAN号和网络号之间都是对应的。VLAN中的PC通过Cisco3750-E接入到核心交换机，3750-E都是二层配置，三层的配置都在Cisco6506-E上，也就是VLAN间的路由都是通过6506-E完成的。PC的IP地址、默认网关和DNS都是自动从DHCP服务器上获得的，不用手工静态配置。

1. 单位FTP应用需求变化

如图3-2所示，在核心交换机Cisco6506-E2上连接有一台“用户PC”，它是放在服务器区中的唯一一台PC，主要是为了方便用户从FTP服务器上下载和拷贝文件。FTP服务器的计算机名称为“ftpserver”。用户PC和服务器都位于VLAN 2中，因为安全方面的要求，在单位的DNS服务器上没有配置FTP服务器IP地址192.168.2.8对应的域名。也就是访问FTP服务器只能通过在“用户PC”的浏览器的地址栏中输入“ftp://192.168.2.8”，或者输入FTP服务器的主机名称“ftp://ftpserver”，就都可以访问到FTP服务器上的资源。

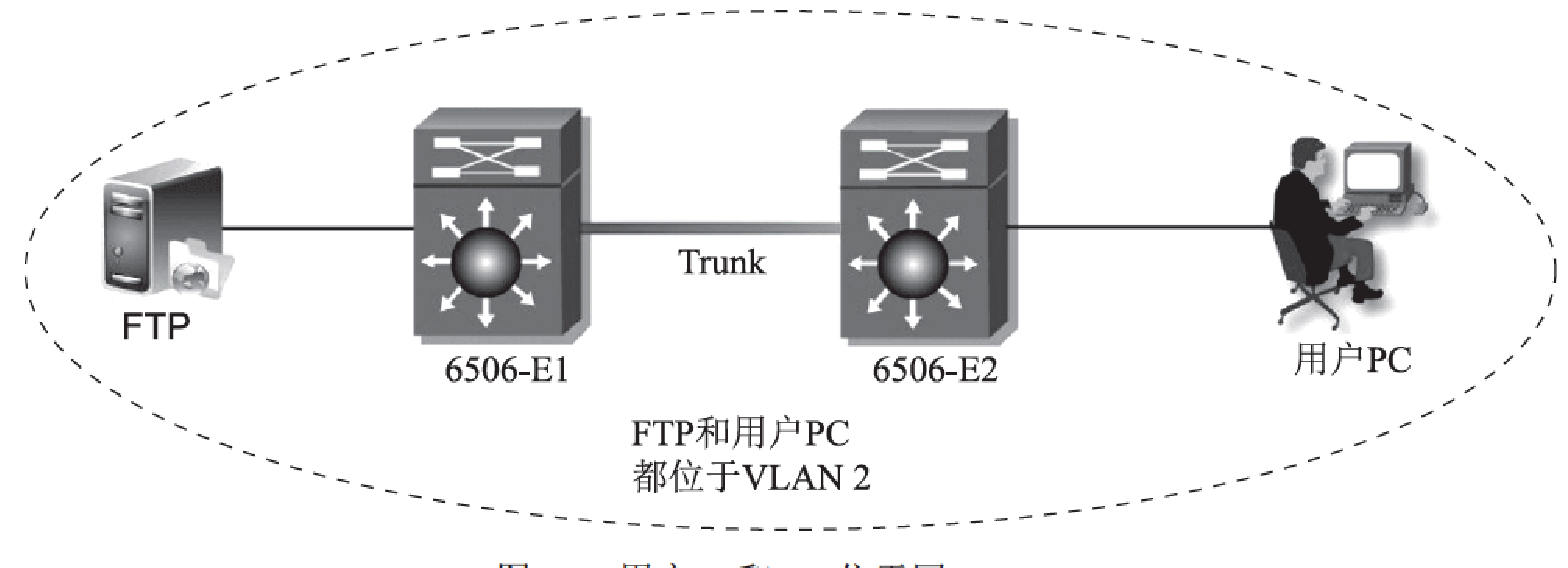


图3-2　用户PC和FTP位于同一VLAN

但是，随着用户业务需求的变化，访问FTP服务器的用户都迁移到了VLAN 102中，原来位于VLAN 2中的“用户PC”被取消掉了。目前，VLAN 102中的PC有一百多台，在图3-3中为了图示的简洁只画出了一台。现在VLAN 102中的用户要访问FTP服务器，只能在PC浏览器的地址栏中输入“ftp://192.168.2.8”才能访问，而用“ftp://ftpserver”则不能访问。因为，VLAN 102中的用户数比较多，让他们都记住192.168.2.8的数字IP地址不是很方便，也容易忘记。所以，还必须满足用户用主机名访问FTP服务器的需求。

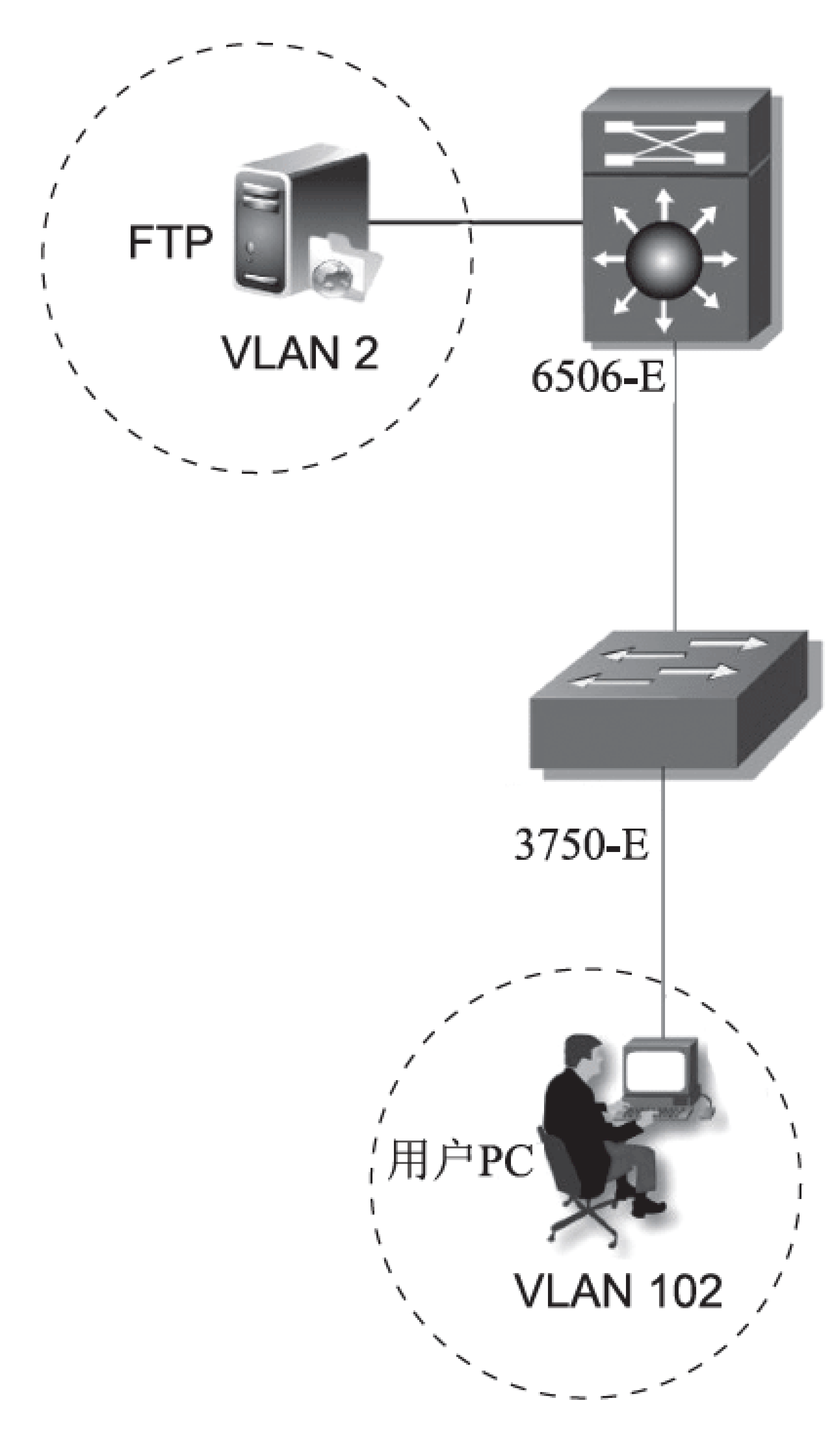


图3-3　用户PC和FTP位于不同VLAN中

2. 配置HOSTS文件满足应用需求

位于同一VLAN 2中的用户PC能用ftp://ftpserver访问FTP服务器，因为PC和服务器都使用Windows系统，默认情况下，它们都位于Windows的“WORKGROUP”的工作组中，Windows也就能把机器名“ftpserver”解析成“192.168.2.8”的IP地址。

但当PC和服务器位于不同VLAN中，虽然默认情况下，PC和FTP服务器也还是位于“WORKGROUP”工作组中，而且位于VLAN 102中的PC通过ftp://192.168.2.8还能访问FTP服务器。但因为两台设备分别位于不同VLAN中时，此时VLAN 102的PC上的Windows系统已经不能把“ftpserver”解析为“192.168.2.8”，也就是用户不能再使用ftp://ftpserver访问FTP服务器上的资源了。

不过，此时利用HOSTS文件的功能，也能解决此问题。默认情况下，在用户电脑的“C:\windows\system32\drivers\etc”目录中找到HOSTS文件。在系统Windows 2000中，应该在“C:\winnt\system32\drivers\etc”目录中。双击HOSTS

文件，然后选择用“记事本”程序打开。之后就会看到HOSTS文件的所有内容了。默认情况下只有一行内容“127.0.0.1 localhost”，其他前面带有“#”的行都不是真正的内容，只是帮助信息而已。将“192.168.2.8 ftpserver”添加到HOSTS文件中。具体格式是先写IP地址，然后空格接服务器的计算机名称。设置完毕后，保存HOSTS文件的配置。这样在访问“ftp://ftpserver”时，PC就会根据HOSTS文件，把地址解析为“ftp://192.168.2.8”，也就可以访问FTP上的资源了。

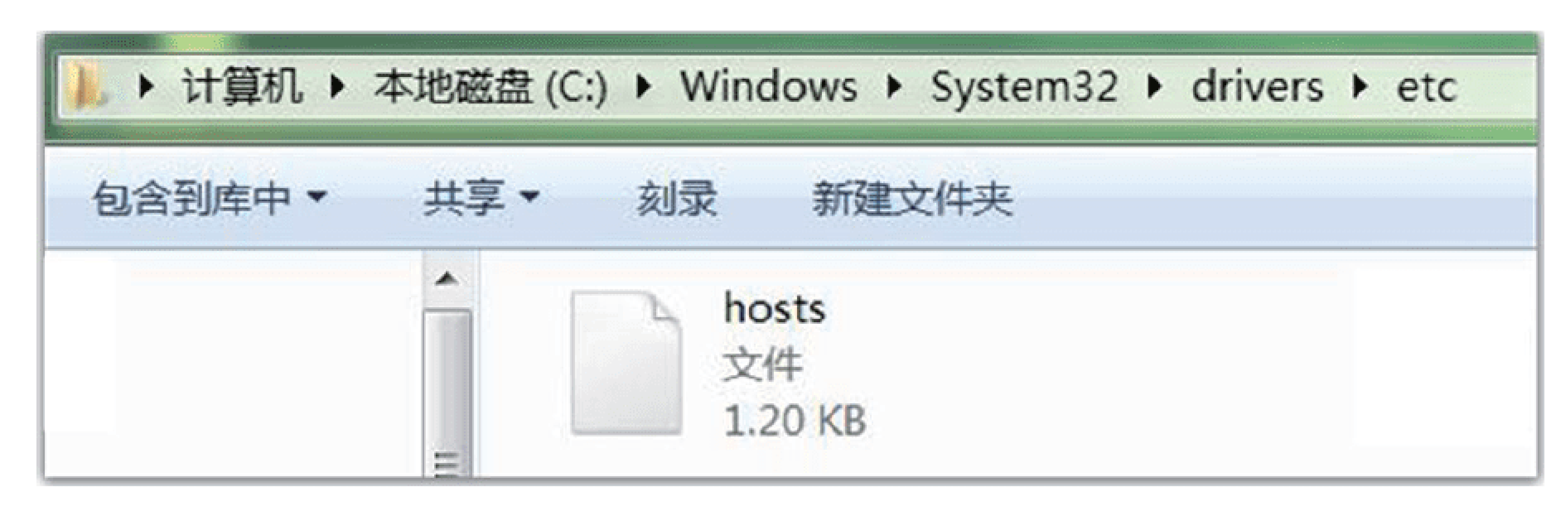


图3-4　hosts文件在windows系统中的位置

3. 总结

(1)在Windows系统中，NetBIOS使用广播进行通信，而广播是无法通过路由器的。也就是两个子网没法通过NetBIOS进行相互通信。但若是在子网当中架设了WINS服务器的话，就可以解决此问题。WINS服务器为NetBIOS提供名字注册、更新、释放服务，并在需要时将它解析成为IP地址。

所以，在三层交换机中，开启了三层功能后如果不用ACL限制VLAN之间的通信，各个VLAN之间是连通的。这样，同一VLAN内部的机器能在“网上邻居”中看见对方，不同VLAN之间的机器不会出现在“网上邻居”中。但是如果在网络中架设了WINS服务器，就可以在“网上邻居”中看见不同VLAN之间的PC。

(2)DNS(Domain Name System，域名系统)目前已普遍应用到企业网络中，它是由解析器和域名服务器组成，保存有该网络中所有主机的域名和对应的IP地址，并具解析功能。其中域名必须对应一个IP地址，而IP地址不一定要有域名。在互联网中域名与IP地址之间是一对一或者多对一的关系。

DNS实现的是IP地址和域名的映射，而WINS服务器功能实现的是IP地址和计算机名称的映射，它集中管理计算机名称和IP地址。通常这些计算机名称都是

在某个单位内部有效，例如，在一个局域网内可以通过使用计算机名访问另一台计算机。访问时就有一个查询IP地址的过程，这就是通过WINS服务来实现的。

(3)HOSTS是一个没有扩展名的系统文件，可以用记事本等工具打开，其作用就是将一些常用的网址域名与其对应的IP地址建立一个关联“数据库”，当用户在浏览器中输入一个需要登录的网址时，系统会首先自动从HOSTS文件中寻找对应的IP地址，一旦找到，系统会立即打开对应网页，如果没有找到，则系统会再将网址提交DNS域名解析服务器进行IP地址的解析。

HOSTS文件在不同操作系统，甚至不同Windows版本的位置都不大一样，Windows XP和Windows 7/8系统默认位置在“Windows\System32\drivers\etc”。Win7系统有时需要提升用户对HOSTS文件的操作权限，否则打不开HOSTS文件。具体方法是：按着Shift键，然后在HOSTS文件上面右击，以管理员方式运行即可。一般来说用户访问互联网，比如访问百度或新浪，要首先通过DNS服务器把要访问的网站域名解析成一个唯一的IP地址。之后浏览器才能对此网站进行定位并且访问其数据。

操作系统规定，在进行DNS请求以前，先检查系统自己的HOSTS文件中是否有这个域名和IP的映射关系。如果有，则直接访问这个IP地址指定的网络位置，如果没有，再向已知的DNS服务器提出域名解析请求，也就是说HOSTS的IP解析优先级比DNS要高。

总的来说HOSTS文件有三大方面的功能：一是加快域名解析。对于要经常访问的网站，我们可以通过在HOSTS中配置域名和IP的映射关系，提高域名解析速度。由于有了映射关系，当我们输入域名计算机就能很快解析出IP，而不用请求网络上的DNS服务器。二是方便局域网用户。在很多单位的局域网中，会有服务器提供给用户使用。但由于局域网中一般很少架设DNS服务器，访问这些服务器时，要输入难记的IP地址。这对不少人来说相当麻烦。可以分别给这些服务器取个容易记住的名字，然后在HOSTS中建立IP映射，这样以后访问的时候，只要输入这个服务器的名字就行了。三是屏蔽网站。屏蔽网站也就是域名重定向功能。有很多网站不经过用户同意就将各种各样的插件安装到用户的计算机中，其中有些说不定就是木马或病毒。对于这些网站可以利用HOSTS把该网站的域名映射到错误的IP地址或本地计算机的IP，这样就访问不到该网站了。在Windows系统中，约定127.0.0.1为本地计算机的IP地址，0.0.0.0是错误的IP地址。如果我们

在HOSTS中，写入以下内容：

```
127.0.0.1 # 要屏蔽的网站 A
0.0.0.0 # 要屏蔽的网站 B
```

这样，计算机解析域名A和 B时，就解析到本机IP或错误的IP，也就达到了屏蔽网站A 和B地址的目的了。

修改HOSTS文件，就是把HOSTS文件中的DNS解析对应关系进行修改，从而实现正确解析的目的。因为在本地计算机访问某域名时会首先查看本地系统中的HOSTS文件。HOSTS文件中的解析关系优先级大于DNS服务器上的解析关系。 这样当我们希望把某个域名与某IP地址绑定的话，就可以通过在HOSTS文件中添加解析条目来实现。

所以，在VLAN 102中的PC浏览器地址栏中输入“ftp://ftpserver”后，计算机会首先查看HOSTS文件中是否有ftpserver对应的IP地址，若有的话，就按照对应的IP地址访问服务器上的资源。当然，若是在网络中架设了WINS服务器，也可以在VLAN 102中的PC的“资源管理器”的地址栏中，或者是在“运行”中，输入“\\ftpserver”回车，也可以访问到FTP服务器上的资源。两种访问FTP服务器的方法在功能上是一样的，但在实现的原理上是不同的。

3.2　运维实例：用BAT文件提高维护效率

作为一名网络运维师，拿着笔记本电脑跑来跑去排除各种网络故障是常有的事。故障的类型也总是千变万化，有时是客户端故障，有时是网络设备故障。为了确定每一个故障的部位和原因，最常用的方法就是使用替换法。更换一根网线，看故障有没有消失，或者更换客户端的电脑看故障消失没有，若故障消失那就说明是电脑的故障。若故障依然存在，那网络的故障就和客户端的电脑没有关系。但使用替换法，在用一台笔记本电脑替换了客户端的电脑后，通常还要对电

脑进行一系列的设置，以保证更换后笔记本电脑的配置和原来电脑上的配置是一样的。最常见的就是网络参数的设置，如IP地址、子网掩码、默认网关和DNS地址等。但就是这些简单的设置，常常会影响网络工程师排查故障的效率，因为需要来回的设置，耽误了很多的时间。下面就通过一则实例，说明通过巧妙利用BAT的可执行文件，来提高网络运维人员的工作效率。

1. 网络结构说明

目前公司和其他的一些单位(如学校)普遍使用的网络结构都是如图3-5所示的结构，也就是园区网的架构。图3-5中使用的网络设备都是Cisco的设备，在实际部署时H3C和华为的网络设备通常使用的也比较多。在图3-5中为了确保重要设备的稳定性和冗余性，核心层交换机使用两台Cisco4506，它们之间通过Trunk线连接。在接入层使用了多台Cisco2960交换机，图示为了简洁，只画出了两台。在核心交换机上连接有单位重要的服务器，如DHCP、E-MAIL、WEB和视频服务器等。单位IP地址的部署，使用的是A类私有10网段的地址。其中，DHCP服务器的IP地址为10.10.1.1/24。WEB服务器的IP地址为10.10.2.1/24，网络中DNS地址使用的是202.96.96.68和8.8.8.8，子网掩码都是255.255.255.0，网络终端的默认网关地址的前三个数字和终端的IP地址都是一样的，只是最后一个数字为254，如DHCP和WEB服务器的默认网关分别是10.10.1.254和10.10.2.254。

因为网络中有DHCP服务器，所以客户端的IP地址、子网掩码都是从DHCP服务器上自动获得的。而网络中连接在核心交换机上的服务器IP地址、子网掩码等网络参数的配置都是通过静态手工配置的，而不是从DHCP服务器上自动获得的。一般网络中的客户端和服务器的网络参数都是这样配置的，因为服务器的网络参数一般都是固定使用的，很长时间都不会发生变化，若经常变化的话，也会影响到服务器的应用系统的相关配置。另外，若是服务器上的IP地址变化的话，和IP地址相对应的域名往往也要做相应的调整，所以服务器上的网络参数一般都是静态配置的。但是对于网络中客户端的电脑，方便性往往是其首先要考虑的，若让用户经常自己手动配置IP地址，那是比较麻烦的，自动从DHCP服务器上获取网络参数才是最好的解决方案。

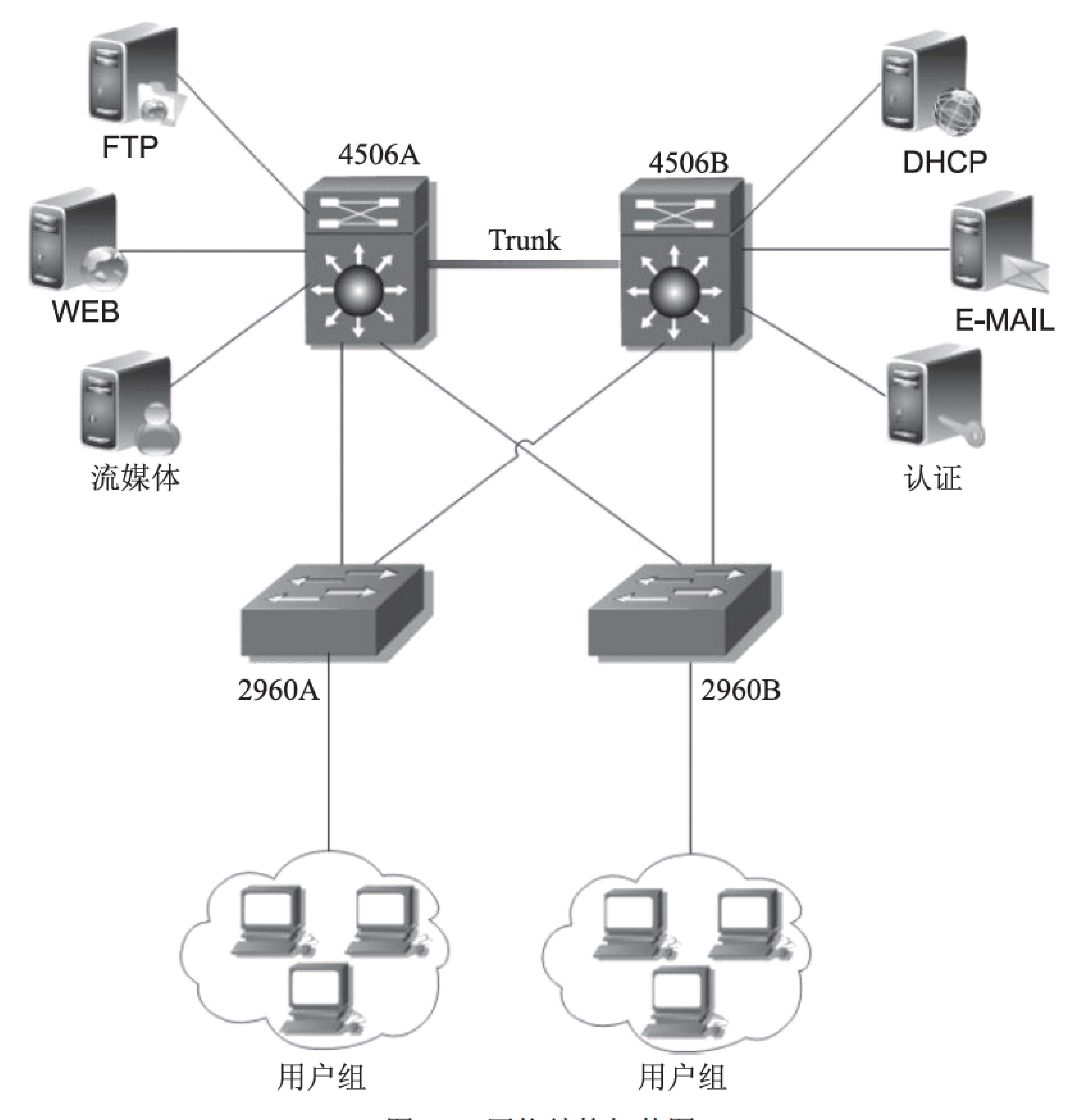


图3-5　网络结构拓扑图

2. 排除网络故障经常遇到的问题

在网络中，常常会出现用户不能访问服务器上应用系统的故障。例如，在图3-5的网络中就可能会出现这种故障。“用户组”中的一台PC不能访问WEB服务器上的应用，而且在PC上也不能ping通WEB服务器。PC的IP地址、子网掩码、默认网关和DNS地址都是从DHCP服务器上自动获取的。

发生故障的原因可能是PC或者是WEB服务器有问题，也可能是网络设备或者网络线路有问题。若是不能马上定位故障发生的部位，最好的解决办法就是利用“替换法”。把不能访问WEB应用的PC用一台笔记本电脑代替，然后看故障有没有消失，故障消失的话就说明是用户PC的故障，否则故障就和PC没有关系；或者用笔记本电脑代替WEB服务器，然后再在用户组的PC上看能不能ping通代替WEB服务器的笔记本电脑，能ping通就说明网络不通的问题和WEB服务器有关，否则和WEB服务器无关。

这种排除故障的方法，有一个不方便的地方就是要频繁的在电脑(Windows 7系统)的“开始”→“控制面板”→“网络和共享中心”→“更改适配器设置”→双击“本地连接”→双击“Internet协议版本4(TCP/IPv4)”中进行各项网络参数的配置，如图3-6所示。

图3-6　“Internet协议版本4(TCP/IPv4)属性”图示

例如在上面使用“替换法”排除故障的时候，用笔记本电脑替代了WEB服务器，就要在笔记本电脑上，在如图3-6所示的地方，设置和WEB服务器上参数一样的网络配置。若这时又要使用笔记本电脑替代用户组的PC进行测试，就又要把笔记本上网卡的网络参数，在如图3-6所示的上面选择“自动获得IP地址”和“自动获得DNS服务器地址”。这样来回的在如图3-6所示的地方进行网络参数的配置，其实是很繁琐又很耽误时间的，那有没有配置网卡网络参数快捷的方法呢？

3. 利用BAT文件快速配置网卡的网络参数

其实，可以创建两个BAT的可执行文件，来提高配置网卡网络参数的效率。首先新建一个文本文档，然后把如下代码复制粘贴到文本文档中：

```
netsh interface ip set address “本地连接” dhcp
netsh interface ip set dns “本地连接” dhcp
```

然后保存文件，注意保存文件的格式为“.bat”格式，不要保存成“.txt”格式，例如DHCP.bat。再新建一个文本文档，把如下所示的代码复制粘贴到文本文档中：

```
netsh interface ip set address “本地连接” static 10.10.2.1 255.255.255.0 10.10.2.254
netsh interface ip set dns “本地连接” static 202.96.96.68
netsh interface ip add dns “本地连接” 8.8.8.8
```

然后以Net.bat格式保存文件。若这两个文件存放的位置不在电脑的桌面上，可以把它们拷贝到桌面上，方便以后经常的使用。如图3-7所示。

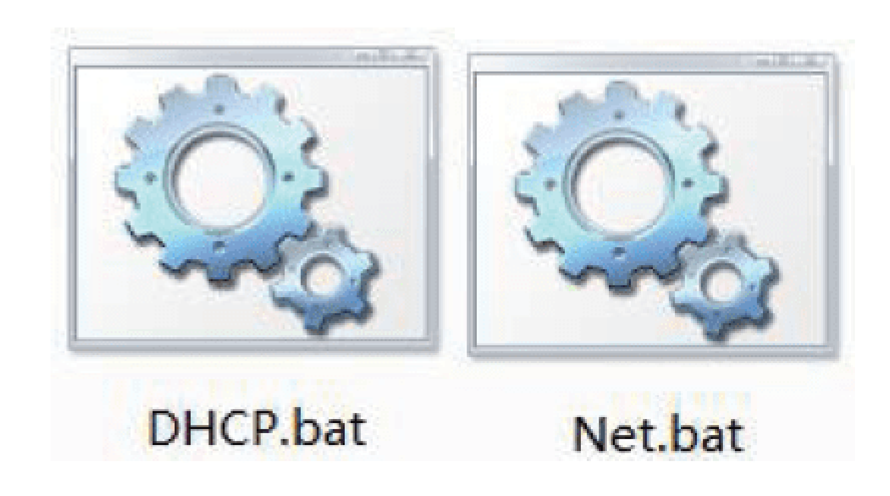


图3-7　桌面上的“DHCP.bat”和“Net.bat”可执行文件

这样，在上面排除故障的过程中，若是想把笔记本电脑网卡的IP地址、子网掩码、默认网关和DNS地址分别设置为10.10.2.1、255.255.255.0、10.10.2.254和“202.96.96.68和8.8.8.8”，直接在笔记本电脑的桌面上双击“Net.bat”的图标，执行“Net.bat”文件即可。程序运行的时间大约也就一两秒，执行完成后，电脑网卡的参数自动就变成了上面的参数。若想再让笔记本电脑网卡从DHCP服务器上自动获取IP地址，只需在电脑的桌面上双击执行“DHCP.bat”的可执行文件即可。

4. 总结

(1)有时配置电脑网卡的网络参数，并不都是和Net.bat文件中所列的参数一样，也可能是别的IP地址或默认网关。这种情况下，也不必在如图3-6所示的“Internet协议版本4(TCP/IPv4)属性”中，配置网络参数，只需在电脑桌面的Net.bat文件上点击右键，选择“编辑”后，就可以对Net.bat文件进行编辑，把IP地址、子网掩码等网络参数修改成你需要的值后，保存文件，并关闭。然后双击“Net.bat”的图标执行它，这样就可以很快的把网卡的网络参数配置成你需要的参数。

这种配置网卡网络参数的方法，比在“Internet协议版本4(TCP/IPv4)属性”中配置要快和方便很多。这样长年累月的下来，也能给从事网络管理和维护的工程师们节省很多时间，同时也提高了他们的工作效率。

(2)上面两个BAT文件中使用的netsh命令，是网络维护人员在网络终端上经常使用的一个网络命令，它也是Windows系统本身提供的功能强大的网络配置命令行工具。它允许从本地或远程显示或修改当前正在运行的计算机的网络配置。

例如，命令“netsh interface ip show address/config/dns”，可以分别查看当前电脑中的IP地址配置和IP地址相关的更多信息、显示DNS服务器的地址；命令“netsh interface ip set address/dns”，可以配置电脑网卡接口的IP地址、默认网关和DNS服务器地址。这也是上面“Net.bat”可执行文件中使用的命令；命令“netsh -c interface dump”，可以查看当前电脑的网络配置文件；命令“netsh interface ip set address ‘本地连接’ dhcp”，是配置电脑网卡自动从DHCP服务器获取IP地址和DNS地址。

3.3　运维实例：简单故障，艰难排查

网络结构图如图3-8所示。核心层交换机使用两台Cisco6506，通过Trunk线连接，汇聚层使用了多台Cisco4006交换机，图示为了简洁，只画出了两台。在核心交换机上连接有单位重要的服务器，如DHCP、E-MAIL服务器、WEB服务器等。Cisco6506和Cisco4006之间也是Trunk连接。6506通过光纤连接至互联网。

因为业务需求，单位要在Cisco6506上接入一台交换机，以便扩展6506上的端口数量。我们使用了一台Cisco2900的交换机和6506直接相连。

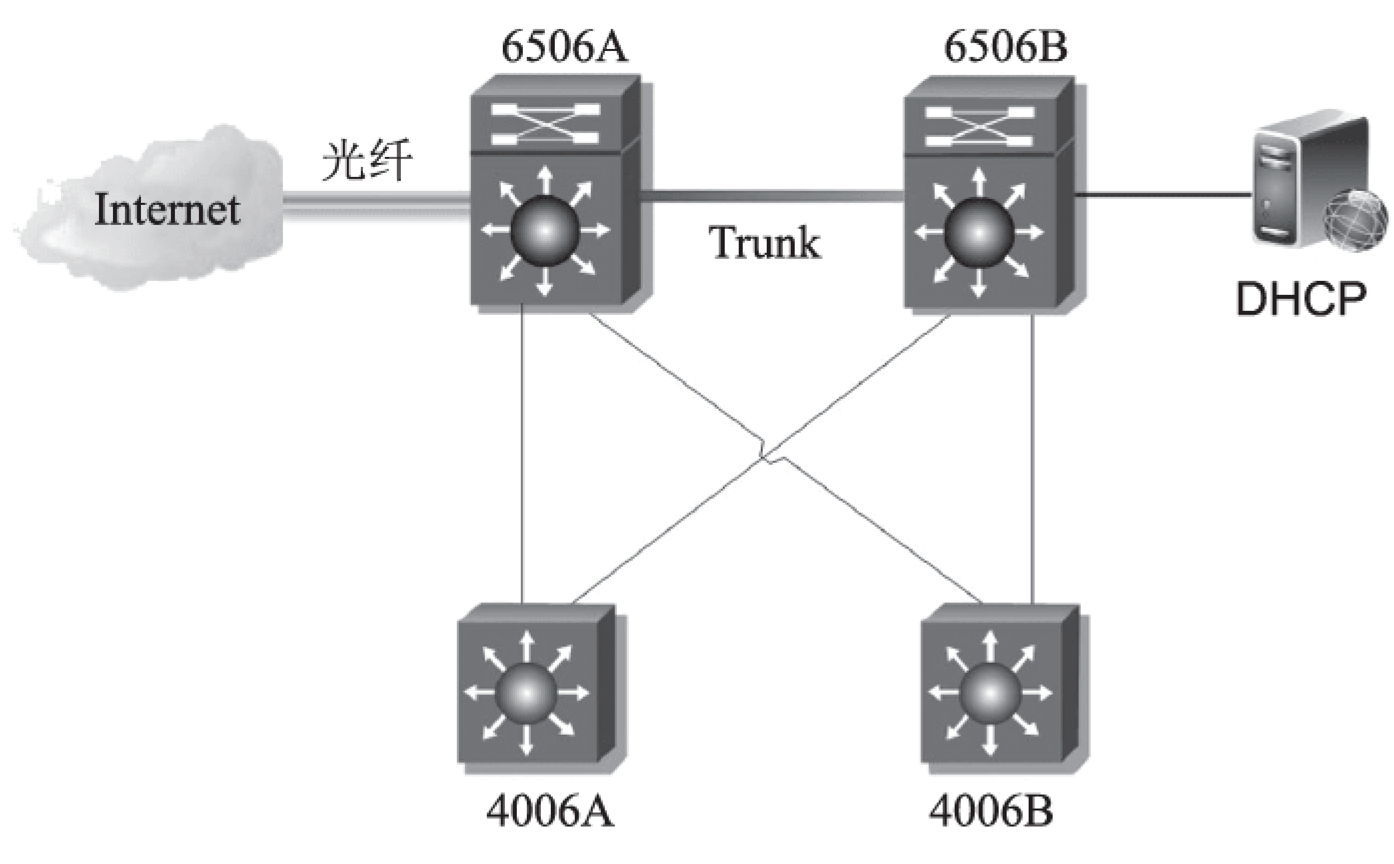


图3-8 单位网络结构图

1. 故障发生的过程

Cisco2900的具体型号是WS-C2924C-XL-EN。Cisco6506上除了引擎板，还有多个模板，主要有两种型号，一种是百兆模板“WS-X6348-RJ-45”，还有一种是千兆模板“WS-X6148A-GE-TX”。因为6506上端口的使用率比较高，没有使用的端口已经很少。正好在6506A千兆模板的G5/48和一百兆模板上的F6/48端口没有使用。

所以，直接使用一根网线，把Cisco2900的F0/1与Cisco6506A的F6/48相连，结果发现用网线连接的两个端口指示灯都不亮。难道这两个端口都故障了，或者是其中一个故障了？

2. 排查故障的步骤

(1)把接入6506A的F6/48端口上的网线拔下来，接入到6506A的G5/48端口上，发现G5/48和Cisco2900的F0/1端口的指示灯都亮，而且接入2900交换机上的PC也可以正常上网。这就确定了2900的F0/1端口没有故障。

(2)为了确认6506A的F6/48端口是否故障，我们又找了另外一台状态良好的Cisco3560交换机，用网线把Cisco3560的F0/1和6506A的F6/48端口相连，结果用网线连接的两个端口的指示灯都亮。在Cisco3560上接入的PC也能正常上网。这就确定了Cisco6506A的F6/48也没有故障。

(3)既然Cisco2900的F0/1和Cisco6506A上的F6/48都没有故障，那为什么用网线连上后，两个端口的指示灯不亮呢。我们想到可能是端口的双工和速率不匹配造成的。接着就把电脑分别接入6506A和2900交换机的CONSOLE口上，把两个端口的各种双工和速率类型都配置了一遍。其中包括最常见的把两个端口的“speed”都配置为100，“duplex”配置为full，但结果端口的指示灯还是没亮。

(4)考虑到Cisco2900的F0/1端口，分别连接到6506A上的G5/48和F6/48，一个正常，一个不正常，所以确定肯定是在这两个端口的设置上有什么不同，造成的这种故障。使用“Cisco6506A> (enable)show port ?”命令后，发现其中有一项是“auto-mdix”，然后分别查看6506A上的G5/48和F6/48有关“auto-mdix”的参数配置，命令如下所示：

```
Cisco6506A > (enable)show port auto-mdix 5/48
Port   auto-mdix
-----    ---------
5/48    enable
Cisco6506A > (enable)show port auto-mdix 6/48
Feature not supported on Module 6.
```

由上面的输出可以看出模板5支持“auto-mdix”功能，而模板6不支持。然后我们用网线再一次把Cisco6506A的G5/48和Cisco2900的F0/1端口相连，并在6506A上把端口G5/48的“auto-mdix”功能关闭，结果两个端口上的指示灯都灭了。到这里基本就确定了是什么地方引起的故障。

(5)查了技术资料后，发现“Auto MDI/MDIX”的功能是“接口自动检测当前连接的网线是直通线还是交叉线，然后根据需要自动进行连接配置”。这时，终于明白故障发生的真正原因。找了一根交叉网线，一端标准是T568A，一端是T568B，然后把6506A的F6/48和2900的F0/1端口相连，结果指示灯显示正常，接入2900的PC也可以正常访问互联网了。

3. 总结

(1)MDI(Media Dependent Interface，介质相关接口)，是指与局域网的传输介质直接连接的规格。使用双绞线电缆的局域网中是RJ-45接头，也就是MDI所指的规格。MDI最初用于规定电缆连接部分的接口，但也用于描述集线器端口插头连线方法。

应该说，连接到端口的设备总要在MDI和MDI-X方式中选择一种。一个发送方发出信号就必须与另一个接收信号的接收方相连，因此，如果某一方采用MDI，连接的另一方就是MDI-X。都是MDI或都是MDI-X是不能正确传输信号的。此外，计算机的局域网网卡和路由器等设备通常采用MDI方式。而集线器的普通端口则采用MDI-X方式连接。

(2)在接口上启用Auto-MDIX功能后，接口就能自动检测出它所需的是直通线还是交叉线，然后再检测当前所使用的连接网线，自动根据连接类型需求进行适当的配置。在不具有Auto-MDIX功能的交换机上，必须使用直通网线连接像服务器、工作站、路由器这类的设备，用交叉网线连接其他交换机或中继器。而支持Auto-MDIX功能的交换机，就可以用任何一种网线连接其他设备，接口可以自动对非正确类型的网线进行纠正。

(3)大部分的网络技术人员都知道，正常情况下路由器和路由器、交换机和交换机之间连接应使用交叉线。但是随着技术的发展，端口都具有了跳线自适应功能，不管你用交叉线还是直通线，这些设备都能自动识别和自动调整的。但是，对于所有的事情都不能想当然，出现上面这种故障时，也要去查看交换机的端口是不是支持这种功能，然后再决定用什么类型的网线。

3.4 运维实例：管理路由和交换设备的3种模式

作为一名网络运维师，在路由器、交换机上进行命令配置，可以说是最为平常的工作，其目的都是通过命令的执行和参数的调整，让路由器和交换机能够以网络运维师的要求去运行。这几乎是网络运维师每天都要进行的操作，那管理网络设备都有哪几种方式，哪种管理方式更简单，哪种方式更高效？这其实主要是

根据网络管理员的实际使用情况进行选择。下面就对网络路由和交换设备的管理模式进行简单的总结。

1. 使用SSH(Secure Shell Protocol，安全外壳协议)方式进行管理

(1)Cisco网络设备的SSH配置。

如图3-9所示为使用SSH方式管理网络设备的拓扑图，Cisco4506和Cisco3750通过Trunk线连接，远程PC通过SSH方式对Cisco4506进行管理，其中Cisco4506是通过端口3/1和Cisco3750的G1/0/25端口相连，两个端口都是光口。PC的IP地址为10.10.20.3/24，并和Cisco3750的G1/0/1端口相连。Cisco4506和Cisco3750上的主要配置如下所示。

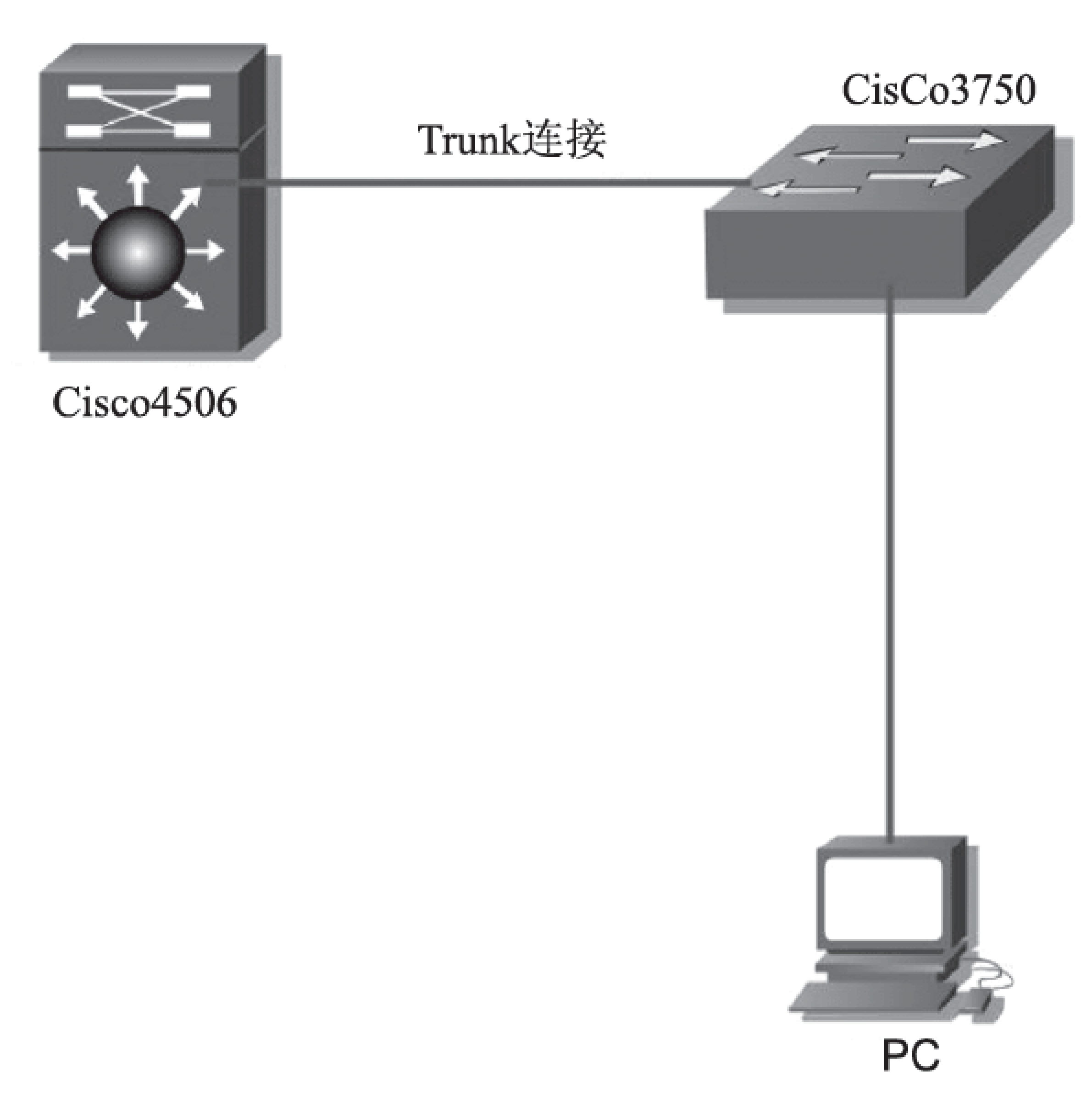


图3-9 使用SSH方式管理的网络拓扑

在Cisco4506上的配置如下所示：

```
interface GigabitEthernet3/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 20,30-300
 switchport mode trunk
```

```
interface VLAN 20
 ip address 10.10.20.1 255.255.255.0
```

在Cisco3750上的配置如下所示：

```
interface GigabitEthernet1/0/1
 switchport access VLAN 20
 switchport mode access
interface GigabitEthernet1/0/25
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 20,30-300
 switchport mode trunk
interface VLAN 20
 ip address 10.10.20.2 255.255.255.0
```

由以上配置可以看出，Cisco4506和Cisco3750的管理VLAN的IP地址分别是10.10.20.1/24和10.10.20.2/24，Cisco3750的G1/0/1端口位于VLAN 20中，并和电脑PC相连。这种情况下，Cisco4506和Cisco3750的三层VLAN 20端口和3750的G1/0/1其实都位于二层VLAN 20中。

要在PC上通过SSH方式管理Cisco4506交换机，还需要在4506上进行如下配置：

```
Switcher(config)# hostname Cisco4506
Cisco4506 (config)# ip domain-name domainname.com
//为交换机设置一个域名，也可以认为这个交换机是属于这个域
Cisco4506 (config)# crypto key generate rsa
```

```
//此命令是产生一对RSA密钥，同时启用SSH，如果你删除了RSA密钥，就会自动禁用该SSH服务
Cisco4506 (config)# aaa new-model
//启用认证，授权和审计(AAA)
Cisco4506 (config)#username cisco password cisco
//配置用户名和密码
Cisco4506 (config)# ip ssh time-out 60
//配置SSH的超时周期
Cisco4506 (config)# ip ssh authentication-retries 2
//配置允许SSH验证的次数
Cisco4506 (config)# line vty 0 15
Cisco4506 (config-line)# transport input SSH
//在虚拟终端连接中应用SSH
```

需要注意的是，在运行上面的配置命令前，要先确认你的交换机和路由器是不是支持SSH功能。一般在交换机或路由器的Enable模式下通过命令“show ip ssh”就可以查看，如在图3-9的Cisco4506中执行如下命令：

```
Cisco4506#sh ip ssh
SSH Disabled - version 1.99
%Please create RSA keys to enable SSH.
Authentication timeout: 120 secs; Authentication retries: 3
```

由上面的输出可以看出，Cisco4506支持SSH功能，只是还没有启用而已。

而在Cisco3750上执行如上命令后会得到如下显示：

```
Cisco3750#sh ip ssh
           ^
% Invalid input detected at '^' marker.
```

由上面的输出可以看出，图3-10中的3750并不支持SSH功能。

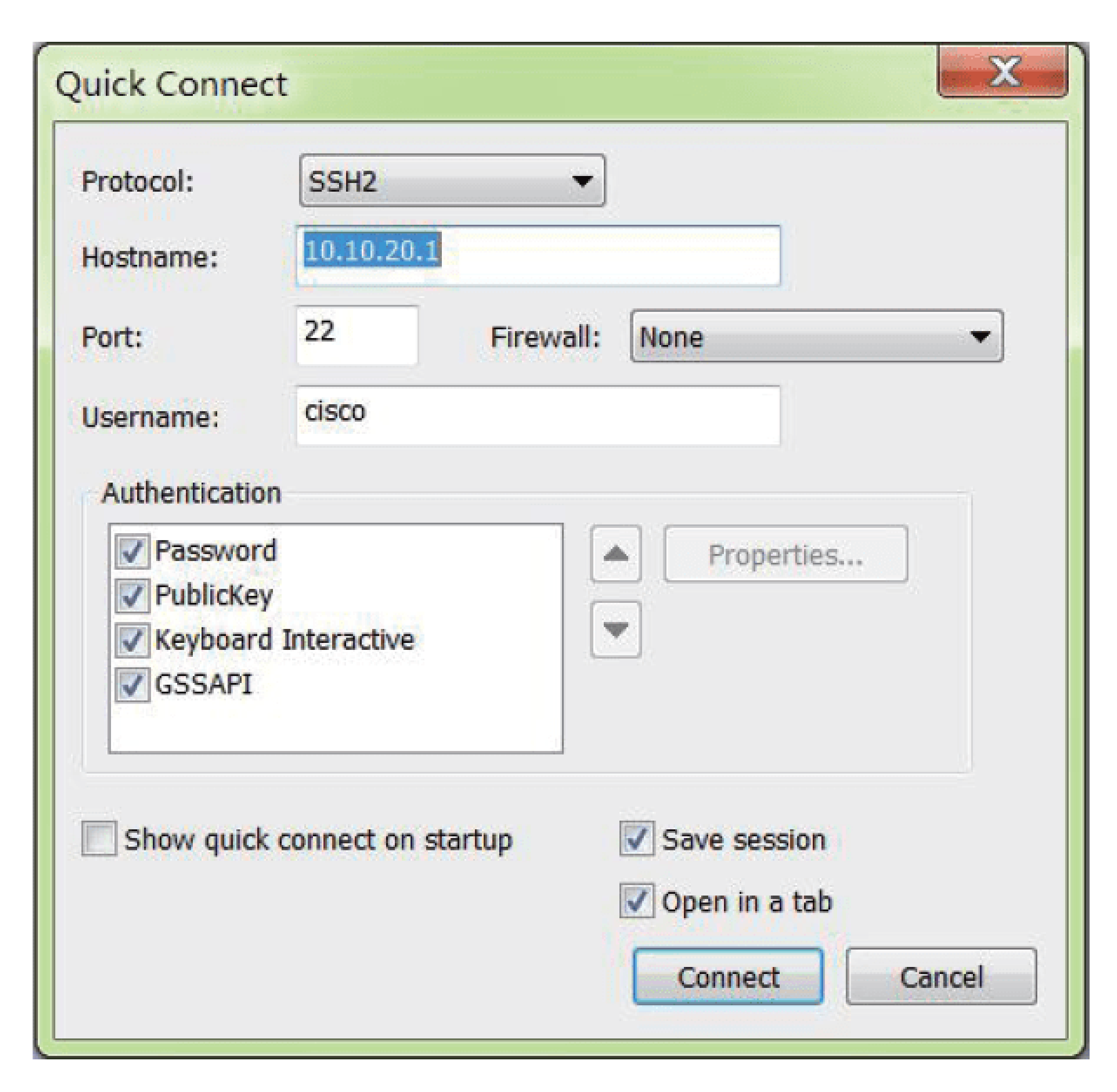


图3-10　虚拟终端上的参数配置

配置完上面的命令后，就可以在电脑PC上测试你的配置。首先，要在PC上安装有SSH终端客户端程序，如SecureCRT，然后在SecureCRT中进行相应的设置，如图3-10所示，然后单击“Connect”按钮，按提示输入用户名cisco及密码cisco，即可进入到Cisco4506交换机的配置界面。

(2)H3C网络设备的SSH配置。

H3C网络设备SSH的配置，在原理上和在思科设备上的配置一样，只是在命令上有差别而已，下面就以H3C S3100-52TP-SI交换机为例，说明如何在H3C交换机上配置SSH。

```
<H3C-S3100> system-view
[H3C-S3100] public-key local create rsa
  //生成RSA密钥对
[H3C-S3100] public-key local create dsa
  //生成DSA密钥对
[H3C-S3100] ssh server enable
//启动SSH服务器
[H3C-S3100] user-interface vty 0 4
[H3C-S3100-ui-vty0-4] authentication-mode scheme
//设置SSH客户端登录用户界面的认证方式为AAA认证
[H3C-S3100-ui-vty0-4] protocol inbound ssh
//设置H3C-S3100上远程用户登录协议为SSH
[H3C-S3100] local-user admin
[H3C-S3100-luser-admin] password simple 12345
[H3C-S3100-luser-admin] service-type ssh level 3
//创建本地用户admin，登录密码为12345，并设置用户访问的命令级别为3，即管理级用户
[H3C-S3100] ssh user admin authentication-type password
//指定SSH用户admin的认证方式为password
```

配置完上面的命令后，也可以使用SecureCRT，用SSH方式登录到H3C S3100-52TP-SI交换机上，输入用户名和密码后，就可以进行管理和配置。

(3)SSH是建立在应用层和传输层基础上的安全协议，也是为解决Telnet的安全隐患而开发的一个协议。因为使用Telnet，在网络上是通过明文传送口令和数据的，“中间人”很容易截获这些口令和数据。而SSH是基于成熟的公钥密码体

系，把所有的传输数据都进行加密，保证在数据传输时不被恶意破坏、泄露和篡改。SSH还使用了多种加密和认证方式，解决传输中数据加密和身份认证的问题，能有效防止网络嗅探和IP地址欺骗等攻击。它也能为远程登录会话和其他网络服务提供安全协议，可以有效防止远程管理过程中的信息泄露问题。使用SSH，还有一个额外的好处就是数据的传输是经过压缩的，所以可以加快传输的速度。SSH还可以为FTP和PPP的使用提供一个安全的“通道”。

SSH协议已经历了SSH1和SSH2两个版本，它们使用了不同的协议来实现，二者互不兼容。SSH2无论是在安全上、功能上，还是在性能上都比SSH1有很大优势，所以目前使用最多的还是SSH2。

2. 使用WEB方式管理网络设备

H3C的路由、交换设备对WEB的管理支持比较好。但在用WEB方式进行管理配置之前，先要对路由、交换设备进行相应的配置。下面就以H3C S3100-8C-SI设备为例说明其相关配置，网络拓扑图如图3-11所示。



图3-11　管理H3C交换机的网络拓扑图

(1)使用一条Console线，把电脑的串口和H3C S3100交换机的Console口相连，配置交换机管理VLAN的IP地址。

```
<H3C> system-view
[H3C] interface VLAN-interface 2
//进入管理VLAN
[H3C-VLAN-interface2] undo ip address
  //取消管理VLAN原有的IP地址
[H3C-VLAN-interface2] ip address 10.10.2.1 255.255.255.0
  //配置以太网交换机管理VLAN的IP地址为10.10.2.1
```

(2)通过Console口，在交换机H3C S3100上配置欲登录的WEB管理用户的用户名和认证口令。添加以太网交换机的Web用户，用户级别设为3，即管理级别的用户。

```
[H3C] local-user admin
//设置用户的用户名为admin
[H3C-luser-admin] service-type telnet level 3
//设置用户级别为3
[H3C-luser-admin] password simple admin
//设置用户admin的密码为admin
```

(3)配置交换机到网关的静态路由。

```
[H3C] ip route-static 0.0.0.0 0.0.0.0 10.10.2.254
//网关的IP地址为10.10.2.254
[H3C] undo ip http shutdown
//执行此命令确保http服务运行
```

配置完上面的命令后，就可以在管理PC的浏览器中输入http://10.10.2.1，按回车键后，就可以看到如图3-12所示的H3C交换机WEB管理登录界面，输入用户名和密码，并选择WEB管理界面的语言后回车，就可以看到如图3-13所示的管理界面，根据管理界面中的语言提示，就可以对交换机H3C S3100中的各项参数进行配置。

需要注意的是，管理PC和H3C交换机的管理IP的10.10.2.1/24之间必须有可达路由，若路由不可达，那无论在管理PC的浏览器中输入怎样的IP地址也不能登录到H3C交换机的WEB管理界面。要验证在管理PC中到交换机的路由可达性，

可以在管理PC的“命令行”中执行“ping 10.10.2.1”命令，若能ping成功的话，一般来说在管理PC和H3C交换机之间的路由是没有问题的。



图3-12　H3C交换机WEB管理登录界面

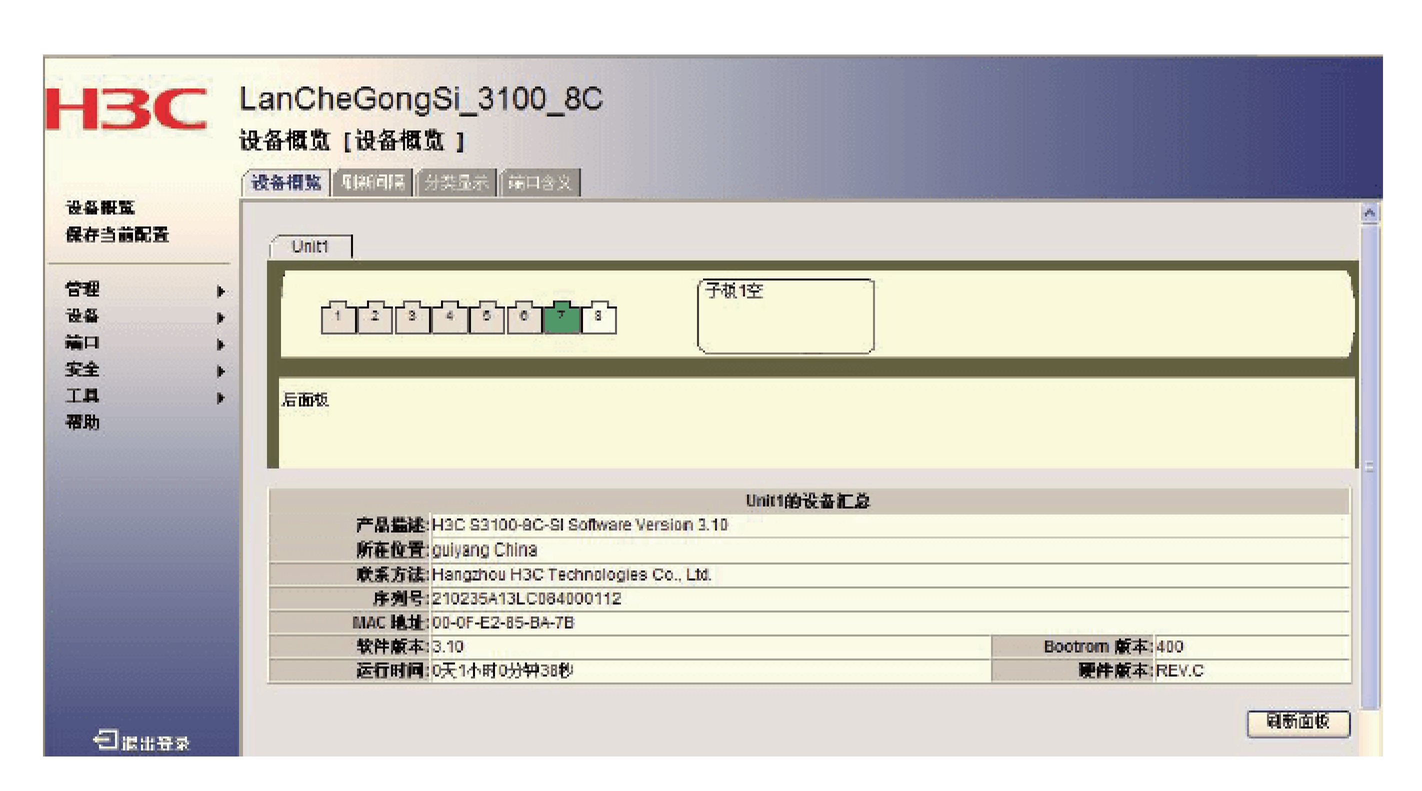


图3-13　H3C交换机的管理配置界面

3. 使用Telnet方式管理网络设备

这种管理模式需要在路由、交换设备上配置的命令比用SSH管理方式配置的命令更少。下面还是以图3-9的拓扑图为例，对交换机进行相应的配置，以便用户通过管理PC，用Telnet方式能够对Cisco4506进行管理配置。

Cisco4506和Cisco3750上的管理VLAN 20的配置和PC的IP地址及其与3750相连端口的配置和“1”中用SSH方式管理的配置都一样，如下所示。

在Cisco4506上的配置如下所示：

```
interface GigabitEthernet3/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 20,30-300
```

```
 switchport mode trunk
interface VLAN 20
 ip address 10.10.20.1 255.255.255.0
```

在Cisco3750上的配置如下所示：

```
interface GigabitEthernet1/0/1
 switchport access VLAN 20
 switchport mode access
interface GigabitEthernet1/0/25
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 20,30-300
 switchport mode trunk
interface VLAN 20
 ip address 10.10.20.2 255.255.255.0
```

要用Telnet方式管理设备，同时还要在Cisco4506上进行如下的配置：

```
line vty 0 15
 password  7  525E0305E3595551E4
 login
```

在Cisco4506和Cisco3750上配置完以上的命令后，也可以使用电脑PC中的SecureCRT软件，Telnet到4506上对其进行管理和配置，在SecureCRT中，需要配置的参数也只有Cisco4506的IP地址10.10.20.1/24，如图3-14所示。

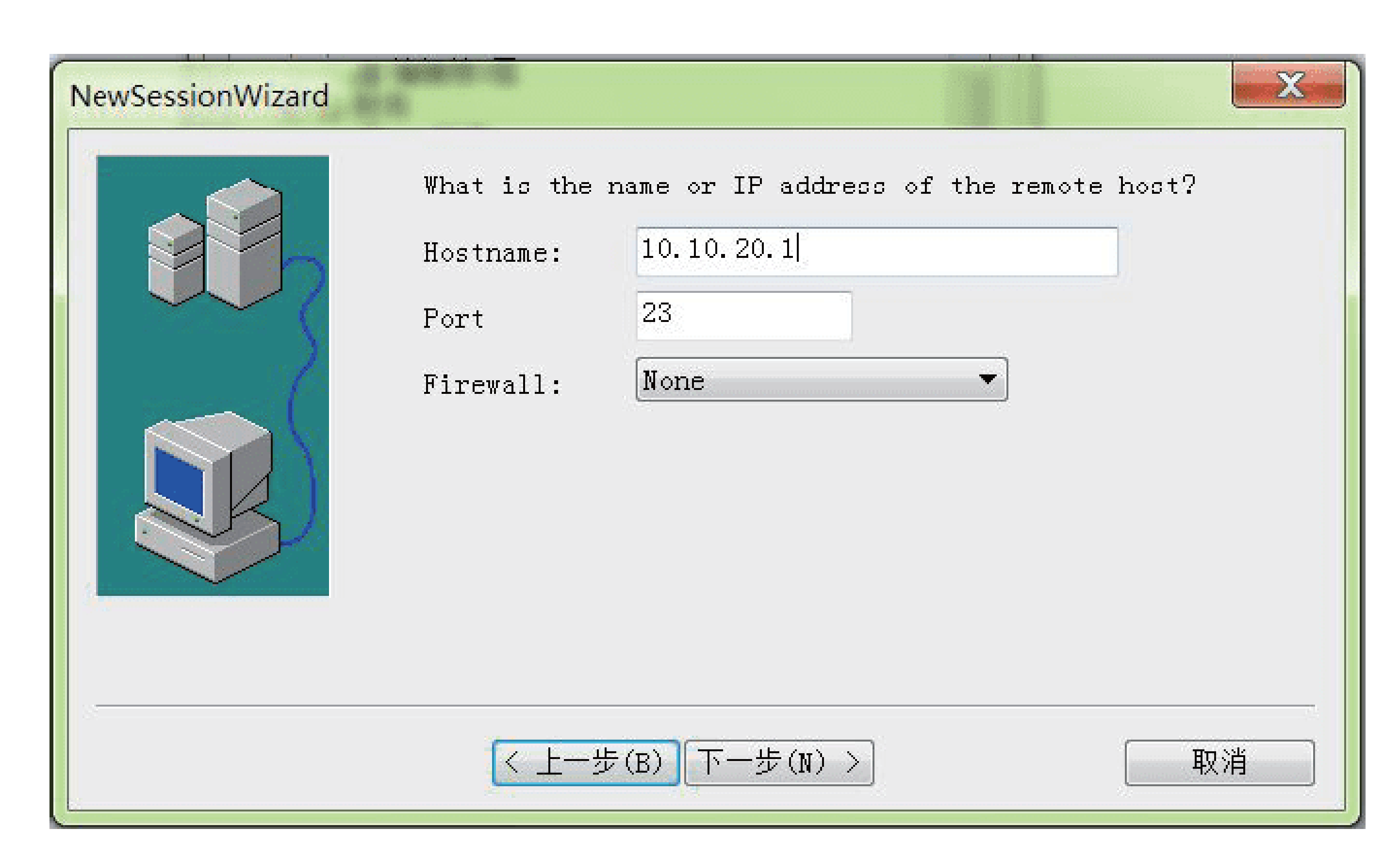


图3-14　在SecureCRT虚拟终端软件上的参数配置

当然，也可以直接在电脑PC的“命令行”中，执行命令“telnet 10.10.20.1”，同样可以Telnet到Cisco4506交换机上对其进行管理和配置。

4. 使用电脑的串口管理网络设备

如图3-15所示的是Cisco3750的正面视图，一般交换机的电口和光口都位于交换机的正面，这种部署方便以后在设备上进行网线和光缆的拔插。而管理配置交换机的Console口一般位于交换机的背面，如图3-16所示。

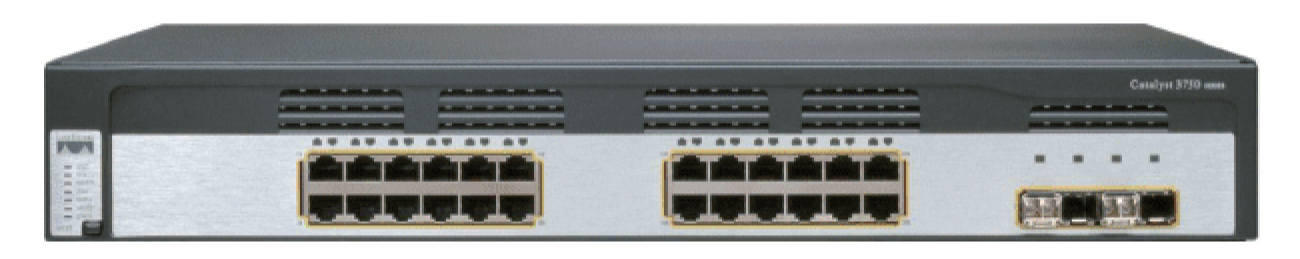


图3-15　Cisco3750的正面视图



图3-16　Cisco3750背面视图及通过Console口配置交换机

通过Console口直接连接到路由器或交换机上，对其进行本地管理配置，也是一种安全、可靠的配置维护方式。当网络设备初次上电、与外部网络连接中断或出现其他异常情况时，通常采用这种方式配置网络设备。

将管理PC 的串口与网络设备的Console口连接，然后在管理PC 上运行终端仿真程序，如Windows系统中的超级终端，或者使用SecureCRT应用程序。然后在终端仿真程序上建立新连接，选择实际连接网络设备时，使用的管理PC上的串口，并配置终端通信的参数。默认情况下的参数都是：9600 波特、8 位数据位、1 位停止位、无校验、无流控。

最后，对路由器或交换机进行上电自检，系统会自动进行配置。自检结束后，系统会提示用户键入回车，直到出现命令行提示符，然后就可以键入命令，配置网络设备，或者查看其运行状态等。

另外，还可以通过配置以下参数，使通过Console口的管理更加安全和符合个性化的需求：

```
line console 0
 exec-timeout 0 0
 password 7 12130F0501595C517E
 logging synchronous
 login
```

命令“exec-timeout 0 0”表示永不超时。若把此命令中的最后一个“0”改为“10”，则表示通过Console口登录后，无操作10秒后就会超时登出。这时若还想登录到交换机，就必须重新输入密码再次进行登录。这种功能可以避免因管理人员短时间离开，回来时还需要重新输入密码。尤其是在密码很复杂的情况下，使用这种命令更有效。但这种功能也存在不安全的因素，所以还是需要按需配置。

命令“logging synchronous”的功能是设置，在输入命令时不会被系统日志消息打断，即阻止烦人的控制台信息来打断你当前的输入，从而使输入的命令更加连续，显得更为易读。

命令“password 7 12130F0501595C517E”的功能，是配置管理PC在通过Console口登录交换机时，必须通过输入密码才能登录，这也是为了防止其他非授权的用户通过Console口访问路由器或者交换机。

5. 总结

(1)从安全角度考虑。首先，使用串口管理网络设备，是最安全的方式，因为它是用电脑和设备直接相连，而不是通过远程登录到设备上。配置的命令和关键性的口令只在设备和电脑之间直接传输，而不会通过其他的网络设备，这也从根本上杜绝了一些“中间人”的攻击。其次，若是使用SSH方式远程登录管理网络设备，也是比较安全的方式，因为SSH协议对所有的数据都进行了加密处理，而不是以明文的方式在网络上传输，若是对安全性要求很高的话，还可以结合SSH使用专门的认证服务器，结合公钥和私钥体制，也可以消除“中间人”的攻击威胁。最后，WEB管理方式和远程Telnet管理方式一般来说是最不安全的方式，不过WEB方式若是通过HTTPS方式进行管理的话，安全性基本和SSH方式一致。但是用HTTP方式管理，管理用户的电脑和网络设备之间所传输的数据也都是没经过加密的，不推荐使用这种方式。Telnet方式也是不安全的管理方式，目前在很多软件中默认都是不支持Telnet功能的，因为它给用户带来了很多潜在的威胁，像Windows 7默认安装完成后，是不能使用Telnet功能，这也是微软给用户考虑细致、周到的地方。若是用户的网络存在很多的安全风险和漏洞，就一定不要使用Telnet方式管理网络设备。

(2) 从易用性角度考虑。首先，WEB管理方式对网络设备进行管理，全都是以窗口界面进行操作，比较直观、容易理解和掌握。不过，WEB方式提供的可配置操作命令比较少，一般只有很少一部分常用的操作命令可以通过WEB方式操作完成，绝大部分的命令还得以命令行的方式进行配置。所以，一般很少能看到网络高手通过WEB方式对网络设备进行管理配置，他们都是飞速地敲着各种命令，从而让网络设备以他们的要求去运行。

其次，若用户的网络环境非常安全的话，比如是一个小型或中型的局域网，没有和外界的Internet进行连通的话，使用Telnet方式管理网络设备也是非常方便的。因为它需要在网络设备上配置的命令比较少，而且在管理PC上不需要安装特别的终端软件，基本上在Linux系统和Windows系统上都支持Telnet功能，这样就可以在网络中的任何一台PC上对所有的网络设备进行远程管理。最后，虽然WEB管理和Telnet方式易用，但是在目前复杂度不断提高的各种网络环境中，还是推荐用户使用SSH方式对网络设备进行配置，因为安全问题往往就发生在一些不严谨的操作规程当中，一个很小的安全问题很可能会导致全网的崩溃。所以，安全无小事！这句话同样适用于网络管理工作。

3.5　运维实例：一起连接错误，导致网络崩溃

公司有两个完全隔离的网络系统，内网和外网。内网的主要作用是处理一些安全性要求比较高，有保密性的事务。并且，内网上有很多服务器，如DNS、WEB、邮件、人事、档案等服务器，这些服务器对公司业务的正常运转都至关重要，所以一定要保证它们的安全性、稳定性和可靠性。而公司的外网主要是让办公人员访问互联网、在Internet下载资料和外单位联系时使用。

1. 公司网络概况

公司内网的核心层交换机使用的是Cisco4507R，在Cisco4507R上接有多个服务器。内网的接入层交换机使用的是Cisco3750。内网中IP地址使用的是A类私有地址，其中内网的DHCP服务器IP地址为10.1.1.1/24。客户端都是自动从DHCP服务器获取IP地址、DNS和默认网关地址。内网的结构示意图如图3-17所示。

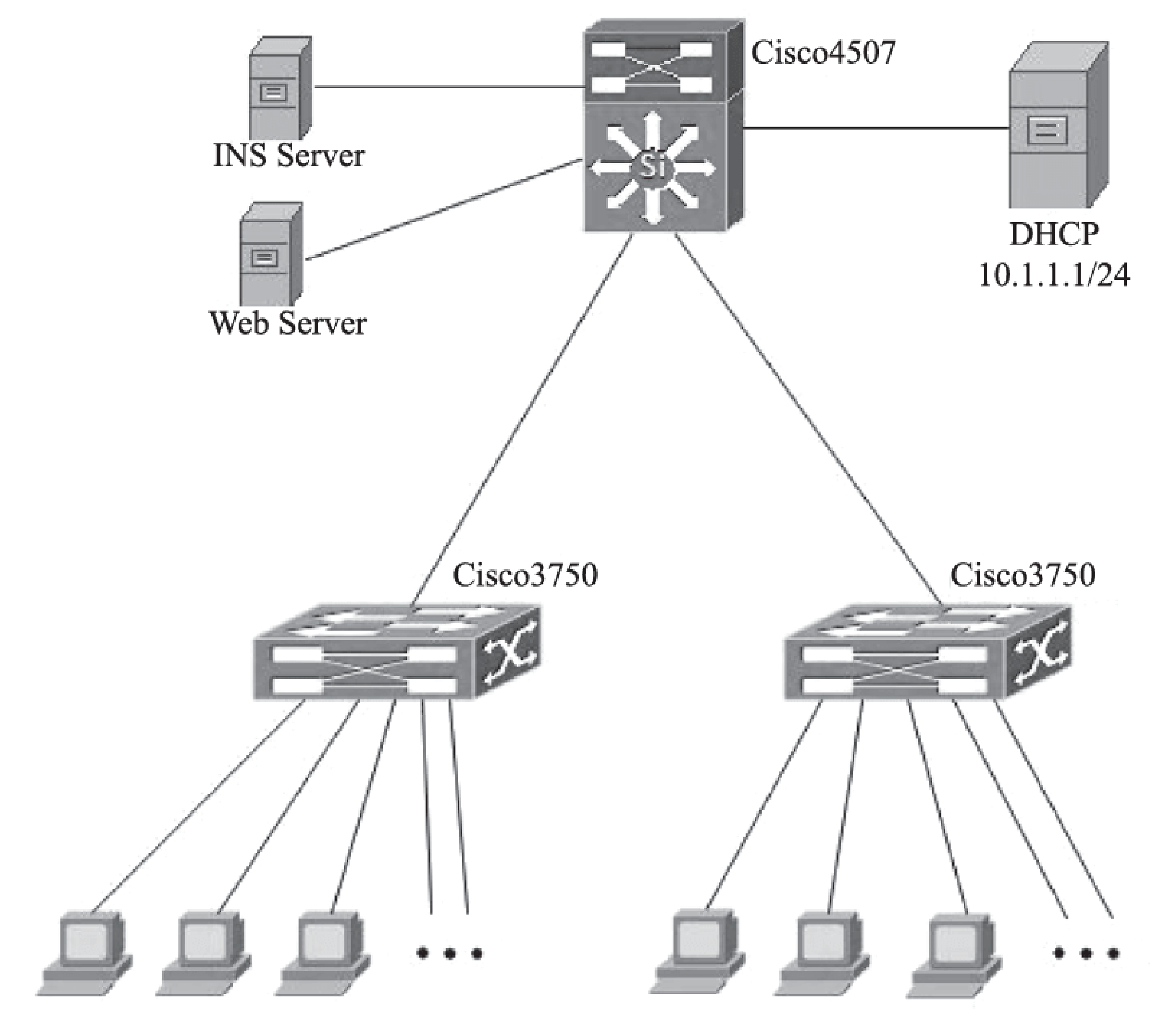


图3-17　公司内网结构图

外网的核心层交换机使用的是Cisco4503。外网的结构相对内网要简单许多，因为只要保证用户能访问互联网就行，在安全性和稳定性方面要求比较低。外网中的接入层交换机使用的是Cisco2960。IP地址使用的是B类私有地址。外网中只使用了一台服务器，即DHCP服务器，IP地址为172.16.1.1/24。同样，外网中的客户端也是自动从DHCP服务器上获取IP地址、DNS和默认网关地址。外网的网络结构图如图3-18所示。

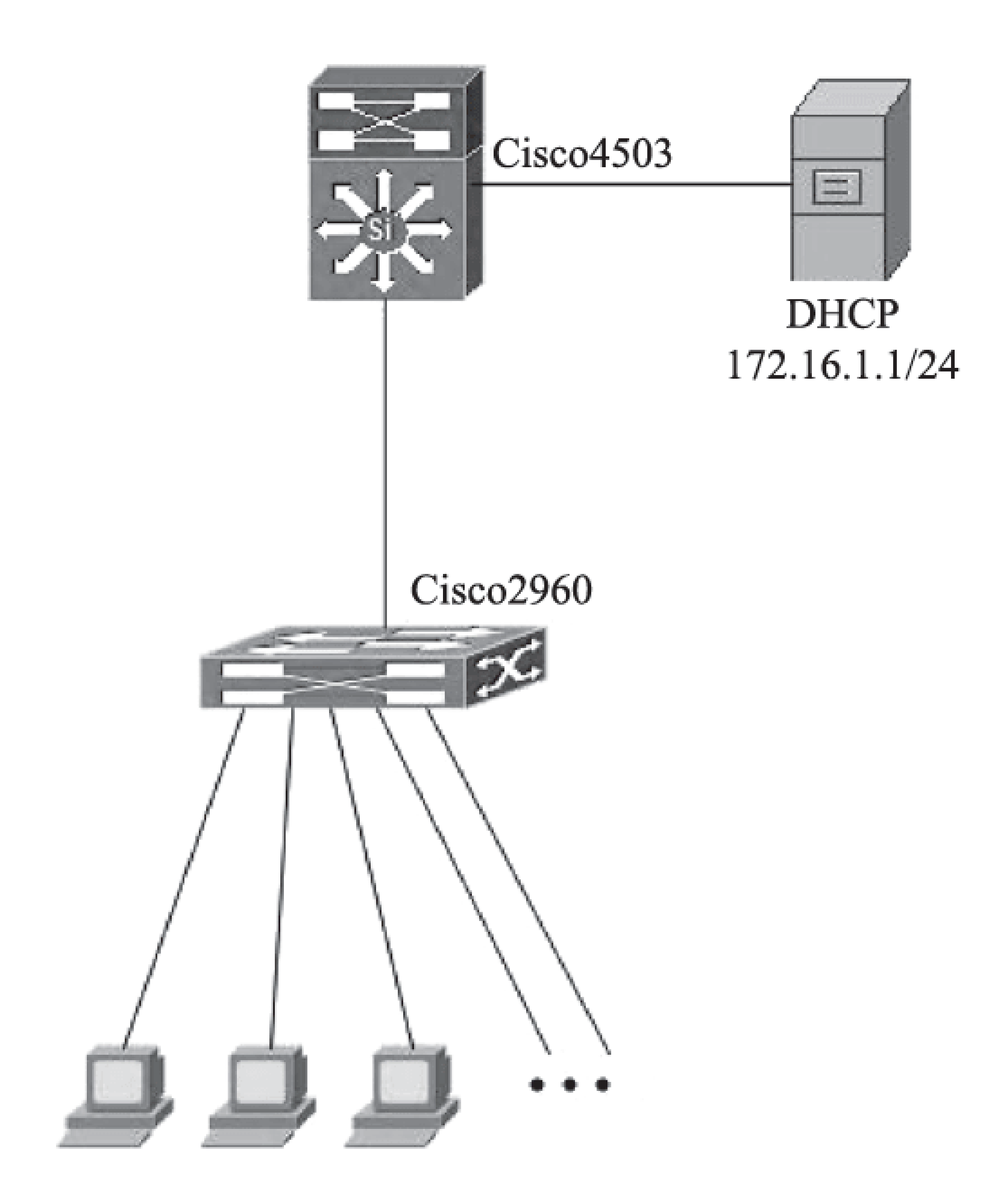


图3-18　公司外网结构图

2. 故障发生的过程

公司的内网和外网在客户端接入时，有的办公室要接入网络中的电脑数量比房间中的信息点数量要多。这样如果不扩展房间中信息点数量，就不能保证所有的电脑都连接到网络中。在这种情况下，我们使用了TP-Link的8端口交换机。交换机的一个端口上连到办公室内网或外网中的一个信息点上，这样交换机上的其他7个端口就可以直接连接到用户的电脑上，有效地扩展了办公室中信息点的数量。

引起网络崩溃的错误连接发生在同一个办公室中。错误连接的示意图如图3-19所示。因为这个办公室中的内网和外网的信息点都很少，所以在用户接入内网和外网时，都使用了一个TP-Link的8端口交换机。发生故障前，办公室一用户

发现自己的电脑不能访问互联网，就在不明白网络运行原理的情况下，看到房间中有两个TP-Link交换机，错误的认为是因为这两个小交换机没有连接起来而引起的故障，就找了一根网线，把两个TP-Link交换机连了起来，结果导致公司内网和外网大面积的网络崩溃。

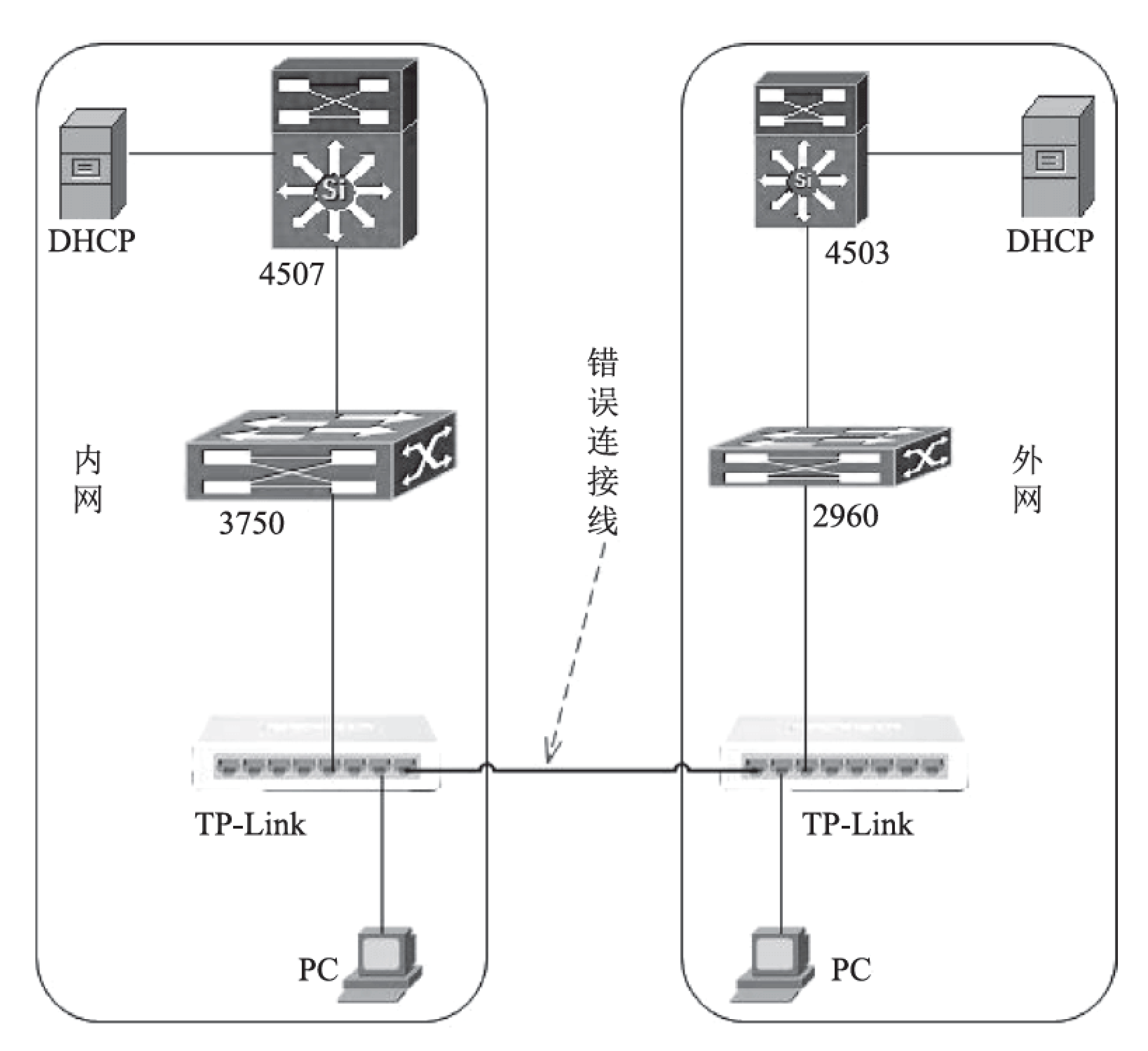


图3-19　引起网络崩溃的错误连接示意图

3. 故障发生的现象和故障的排除

(1)故障发生的现象。故障发生后，很多用户打电话说不能访问网络。有的不能访问内网，有的不能访问外网。到故障现场查看不能正常访问的电脑后，发现内网中的电脑获取到的都是外网的IP地址，即172开头的地址。而外网中的用户获取到的都是内网的IP地址，即10开头的地址。所以我们根据故障现象，初步断定是哪个办公室中把内网和外网连接到了一起。

(2)故障的排除。确定了发生故障的原因后，下一步就是找出在哪个办公室中把内网和外网连接到了一起。但是，可能引起错误连接的办公室有好几十个，总不能一个一个去排查，这样效率太低。

后来，我们在机房中，逐一拔掉连接配线架端口和交换机端口的每根网线，

若拔掉某个办公室配线架上的网线后，公司的网络恢复正常，那就是这个办公室中把内网和外网连接到了一起。后来我们用这种办法找到了引起错误连接的那个办公室，和开始的推测完全一样，确实有人私自把内网和外网的两个TP-Link连到了一起。把错误的连接断开后，公司网络全部恢复正常。

4. 总结

(1)DHCP服务器的工作过程。当一台电脑第一次接入到配置有DHCP服务器的网络中时，客户机上没有任何的IP数据设定，也就是没有IP地址、DNS和默认网关地址，这时它会向网络中发出一个 DHCP Discover数据包。因为客户端还不知道自己属于哪一个网络，所以数据包的源地址为0.0.0.0，而目的地址则为255.255.255.255 ，向网络进行广播。当客户端将第一个 DHCP Discover数据包送出去之后，在一秒之内若没有得到响应的话，就会进行第二次 DHCP Discover数据包的广播。若一直得不到响应的情况下，客户端一共会有4次 DHCP Discover数据包广播。

在DHCP服务器收到DHCP Discover发现报文后会做出响应，它从尚未出租的IP地址中挑选一个分配给DHCP客户机，并根据DHCP Discover数据包中原来携带的客户机MAC地址，向客户机发送一个包含出租的IP地址、DNS和默认网关地址的DHCP Offer提供报文。

如果网络中有多台DHCP服务器向客户机发来DHCP Offer提供IP地址，则客户机只接受第一个收到的DHCP Offer报文提供的IP地址。

(2)深入分析导致网络崩溃的原因。从以上分析DHCP服务器的工作过程可以看出，当网络中有两个DHCP服务器运行的时候，客户机获取IP地址时，哪个DHCP服务器提供的速度快，客户机就采用那个DHCP服务器的提供的IP地址。所以，当把两个TP-Link交换机连接起来后，内网和外网打通，成了一个整体的大网，并且网路中包含两个DHCP服务器，这样内网中的电脑可能获取到的是外网的IP地址，而外网中的电脑获取到的可能是内网的IP地址。结果就导致了整个内网和外网的混乱，客户机也就不能正常访问网络了。

(3)故障的经验和教训。首先要加强客户端的管理。用户出现不能访问网络的故障，应当及时向网路管理部门上报，而不应私自处置。其次，应当禁止用户对放置在办公室中的TP-Link交换机上的网线私自接入和拔出。

3.6　运维实例：简单问题，艰难解决

作为一名网络工程师，并不仅仅是坐在电脑前利用远程控制，在交换机、路由器或安全设备上输入、执行一些命令就能完成所有的工作。有时网络运维师的工作更多的是一些体力活，搬着东西跑上跑下是常有的事。下面就通过一则实例，向你呈现网络运维师工作最真实的一面。

1. 需要解决的问题

如图3-20所示，101和102两个办公室，101办公室墙上有一个信息插座，信息插座上有一个网口和一个电话口，型号分别时RJ-45和RJ-11，就是分别接网线和电话线的。目前大部分的办公室，包括家庭中上网使用的都是这种信息插座。不过，在家庭中使用ADSL上网的话，一般是使用电话线插在信息插座的电话口上，电话线的另一头接ADSL猫，然后从ADSL猫的网口上再引出一根网线接到家里的电脑上就可以访问互联网了。

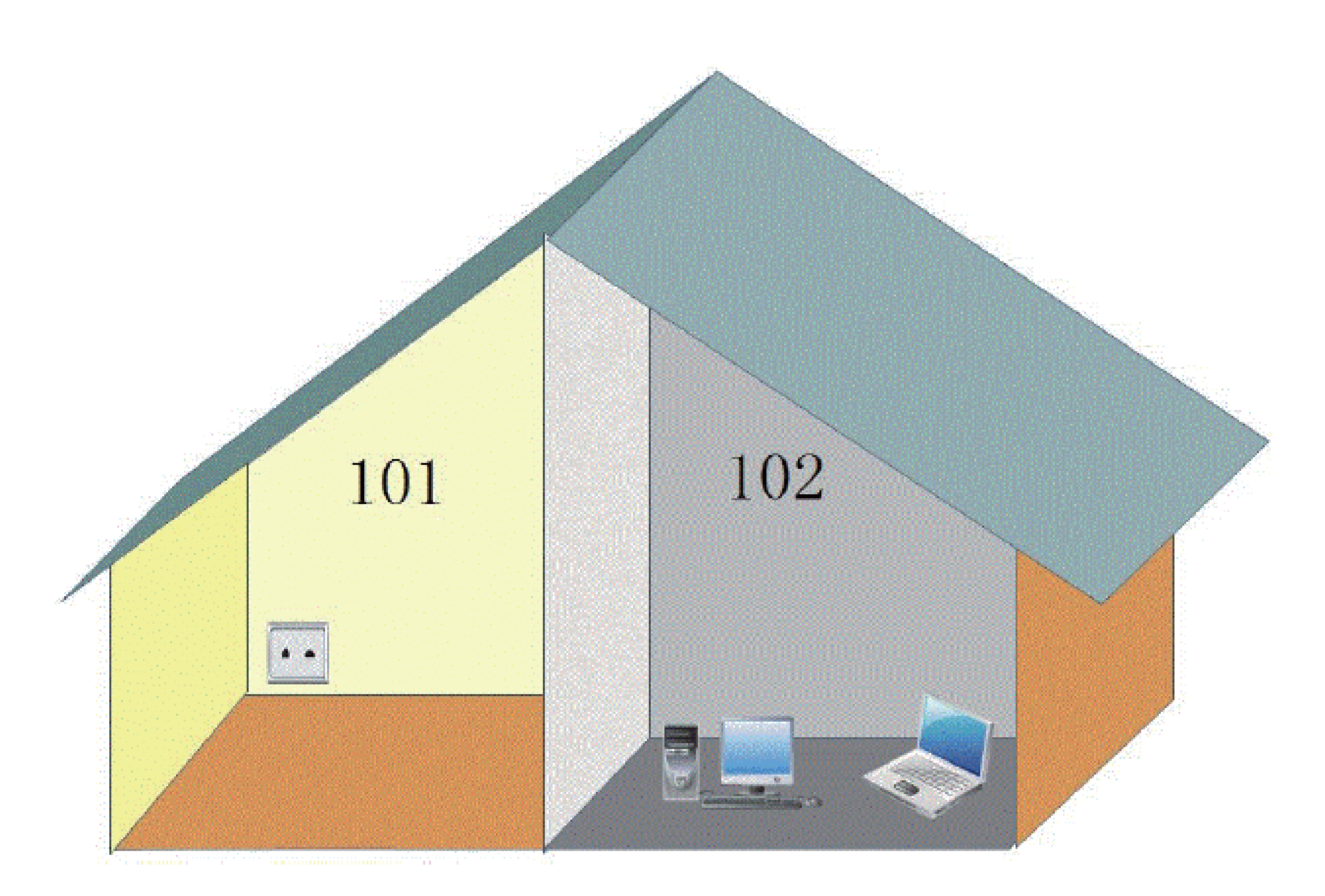


图3-20　需要解决网络问题的图示

但是在单位一般是通过局域网的方式访问互联网的。使用信息插座上的网口，把一根网线的一头接到电脑的网卡，另一头接信息插座的RJ-45口就可以上网了。

从图3-20中可以看出，现在101办公室的墙上有信息插座，用户可以正常访问互联网。但是在102办公室的墙上根本就没有信息插座，所以102办公室的用户就无法上网。造成这种情况，主要是因为102办公室的墙上原来也是有信息插座的，可以通过信息插座的网口访问互联网，不过最近102办公室把内部进行了一次彻底装修，装修时，施工队也许是想偷工减料，也许是没有任何的网络常识，他们装修完后，根本就没有在墙上预留可以上网的信息插座，并且把原来的网线和信息插座口都用水泥给抹上了。

这样做，倒是给装修人员带来了很大的便利，但是给我们网络维护人员却带来了灭顶之灾。现在102办公室的用户需要访问互联网，你说怎么办？

2. 解决问题的几种可能方案

遇到这种问题，我们马上想到了以下三个方案：

(1)方案一，既然现在102办公室没有上网的信息插座，那就重新布线，从办公楼机房的配线架再拉一根网线到102办公室。

但是这种方案很快就被否决了，对于一个已经装修好了的办公室，若要再重新进行布线，那就相当于一个人做整容手术，没做好，要再进行一次整容一样痛苦！所以只能在找其他办法，这种方案不可行。

(2)方案二，方案一中的重新布线是麻烦，但目前101和102两个办公室之间就隔一堵墙。现在在墙上打一个孔，孔不用很大，只要能穿过一根网线即可。

这样102办公室通过墙上的小孔从101办公室扯出一根网线，网线的一头接101办公室墙上的信息插座，另一头接到102办公室，并连上电脑就可以访问互联网了。

但这种方案，很快又被否决了，因为102办公室在装修时，在挨着101办公室的那面墙上，全铺上了一层实木板，不但价格很贵，而且也很漂亮。他们不允许在墙上钻个孔，从而影响整体的美观。

(3)方案三：因为在102办公室装修时，他们预留了电话的信息插座，也就是有电话口，那让用户通过电话线，用一个ADSL猫，不就可以上网了吗。

但是我们单位内部用的是小号电话，也就是和家庭使用的电话系统不太一样。并且单位用户访问互联网都是通过局域网的方式访问的，用户电脑的网卡都

是通过一根网线接到配线架，再通过配线架接到机房的交换机上，然后通过交换机的UPLINK口，再接入到互联网上。用户没有使用过ADSL的方式访问互联网的。

另外，用户若用ADSL访问互联网的话，网速可能会比较慢，这样用户也不会满意。所以这种方法也不能使用。

3. 另外一种方案

其实，还有一种方案，我们在刚开始的时候就也已经想到了，那就是“无线方案”。

无线方案要实施起来，其实也很简单，在101办公室放一个无线路由器，用一根网线，一端接101办公室信息插座上的网口，一端接到无线路由器的WAN口上。然后再拿一个笔记本，用一根网线连接到无线路由器的LAN口上，对无线路由器进行简单的配置，如数据加密的类型，连接到无线网络的用户是否要使用密码等。

然后给路由器加电，在102办公室的用户使用笔记本的话，马上就能上网了，因为现在的笔记本都内置了无线天线。若是使用台式机的话，只需给台式机安装一个USB接口或是PCI接口的无线天线即可，这些设备及它们的驱动程序和无线路由器都是配套的。所以，很快就能把设备安装完成。如图3-21所示，就是最终安装完的示意图。

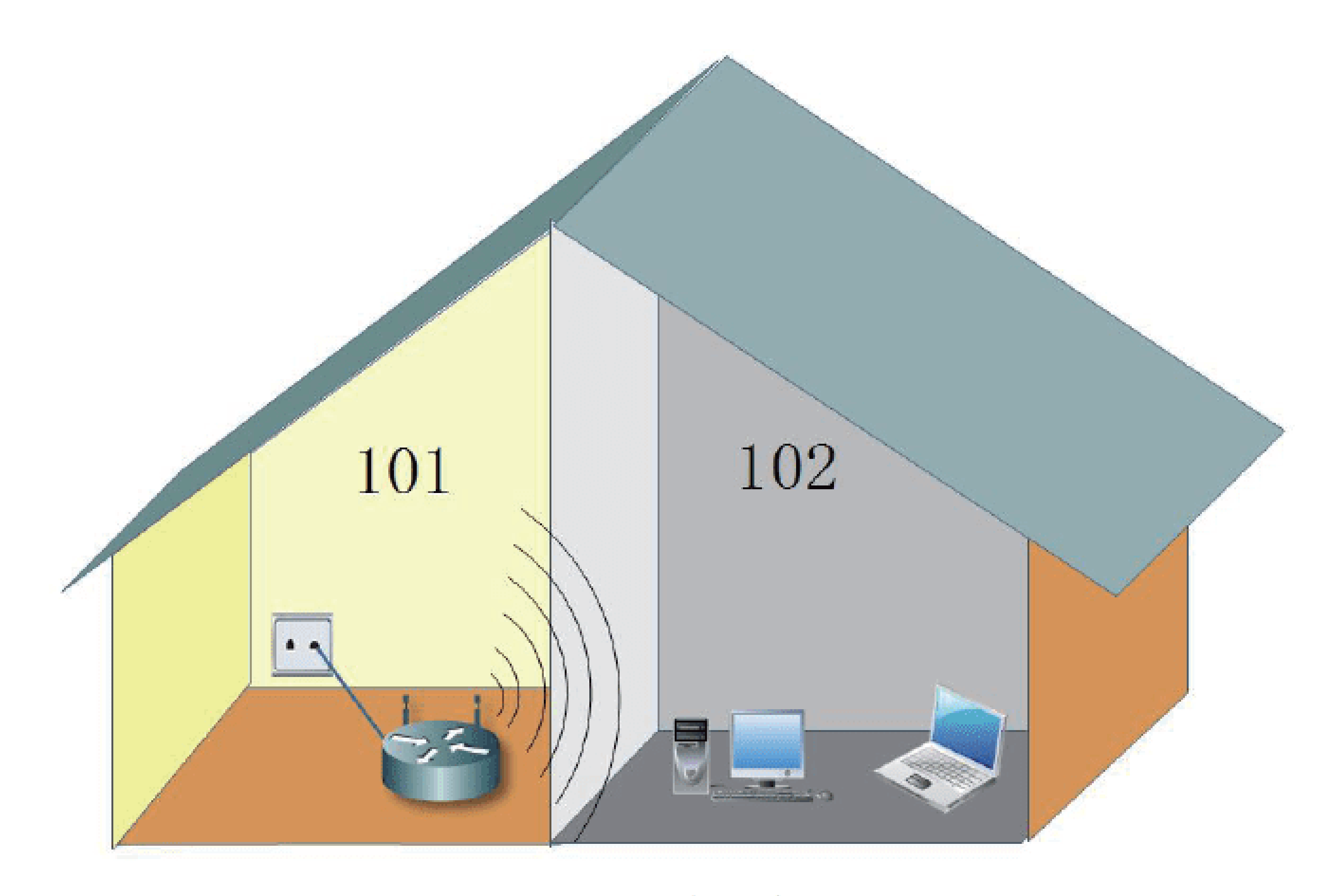


图3-21　无线方案图示

但是这种方案，用户在使用时，总反映信号不是很好，而且还总掉线。知道这种情况后，我们就拿了一台笔记本进行了测试，当笔记本在101办公室使用无

线上网时信号很强，也不掉线。但是当把同一台笔记本拿到102办公室时，无线信号强度确实会变差，上网过程中也会发生掉线。

后来，我们发现在102办公室里，挨着101办公室的那面墙边，摆放了一排铁皮柜，我们觉得可能是这排铁皮柜让无线信号减弱了。然后，我们几个网络维护人员就把那几个铁皮柜搬开，以便无线路由器从101办公室发射到102办公室的信号不被铁皮柜遮挡。

搬开后，用户上网的信号是有所好转，但时不时还是会掉线，很不稳定。后来，我们考虑是不是101和102办公室之间这堵墙，使无线信号减弱了，或者是无线路由器的频率设置有问题？我们想再进行测试，不过要花费的时间比较长。但用户着急要上网，根本没时间让我们做测试，所以我们只能再想别的办法，把问题尽快解决。

4. 最终的解决方案

就在我们觉得不会有什么好办法的时候，突然看到，101办公室和102办公室都有空调在使用，而每个办公室的空调排气管道都是在办公室的墙上钻个洞，通到了室外。

所以，我们想到何不利用空调的通气管道，使用一根长网线，网线的一端连接到101办公室的信息插座上，然后穿过101办公室的空调排气管道，把网线扯到室外，再从室外穿过102办公室的空调排气管道把网线接入到102办公室，然后再接到102办公室的八端口HUB上，再从HUB上引出多根网线接入到用户的电脑上即可，如图3-22所示。

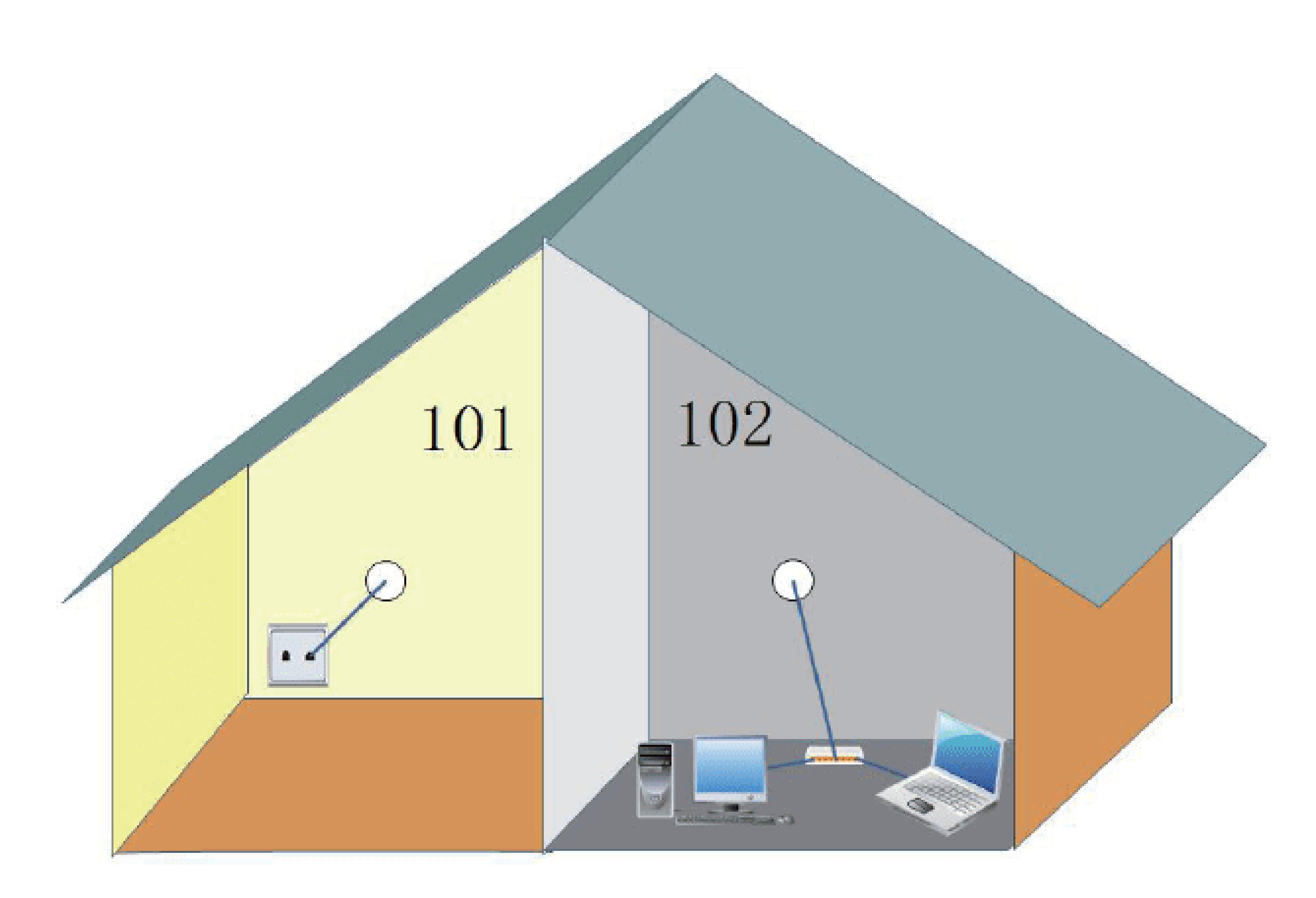


图3-22　最终的解决方案图示

这种方案，使用的设备也比较少，只使用了一根长网线和一个八端口的HUB。而且在使用中，用户反映上网的速度和稳定性都很好。经过大半年的使用，也没有出现掉线和上网速度慢的问题。

5. 总结

(1)一般比较大的单位，在进行办公室或者楼宇的修建时，一定要有技术部门人员的参与和监督。这里的技术人员并不单单指网络方面的技术人员。它包含的范围也比较广，比较常见的，如强电和弱电技术人员。强电主要指单位的供电线路；弱电主要是指单位的电话和网络线路。在招标、施工和验收的各个环节，技术人员都要认真负责，全程参与。有些施工方为了偷工减料，或者觉得甲方人员的技术水平不够专业，就在合同里做了手脚，目的就是为了拿同样的钱而少干点活。这样做的结果常常是给施工方带来了好处，但却给单位的技术人员带来了无尽的麻烦。

因为有时为了在办公室与机房之间架设一根网线，或者在楼与楼之间架设一条光纤，通常要花几天，甚至几个月的时间。这些问题若是在办公室或楼宇刚开始修建的时候，都能考虑全面的话，则会给网络技术人员节省很多的时间。

(2)网络运维师本身的定义和工作的内容需要清晰的界定。现在，大部分从事网络运维师工作的，在单位工作的内容，其实并不单单是网络工作。单位比较小的话，可能网络运维师要把IT部门所有的工作都包了，除了维护单位的网络外，还要维修主机、打印机，维护服务器、应用系统以及负责全方面的工作；比较大的单位可能在业务分配上更专业一点，但也没有达到只从事网络维护工作，只不过不做主机和打印机维修方面的工作，其他的还都要干；只从事网络工作的，可能只是在中国电信、中国联通这样的大单位才能达到。

从专业性和工作的效率上来讲，网络运维师应该只从事和网络有关的工作。可是在现实当中往往并不是这样，大家觉得网络运维师什么都可以干，什么都应该干。网络运维师不仅要解决和网络有关问题，还要解决其他和网络无关的问题。就像上面提到的问题，利用最后一种方案是把问题彻底解决了。我们在把长网线通过空调管道引入到102办公室时，是要有人爬到窗户外边操作的，这很困难也很危险，因为两个办公室并不在一层，都是高空作业，应当要有专业人员去完成的，但现实中都是由网络运维师自己去做的。

这种分工上的不明确，往往会导致工作效率的低下。什么都想做，其实什么都做不好。网络运维师觉得自己只应该做网络方面的工作，而周围的人觉得什么都应该做，结果就是纠纷不断，任何工作都不能高质量、高效率地完成。

若是能界定网络运维师的定义和工作的内容，并得到大家都认可，那就会好很多。目前网络运维师的定义在国内比较权威的定义是："从事计算机网络运行、维护的人员"，而国际上比较权威的定义是："规划、监督、控制网络资源的使用和网络的各种活动，以使网络的性能达到最优"。若网络运维师和网络运维师服务的对象都能按照上面定义要求别人和要求自己的话，那我们网络运维师工作的方方面面就会得到很大的改善。

3.7 运维实例：多台电脑共享上网

公司一办公室开始只有一台电脑通过ADSL Modem上Internet，后来办公室又添了一台电脑，也想通过ADSL Modem上Internet，我就按照图3-23所示把电话线和网线都连接好，只是多使用了一个HUB。

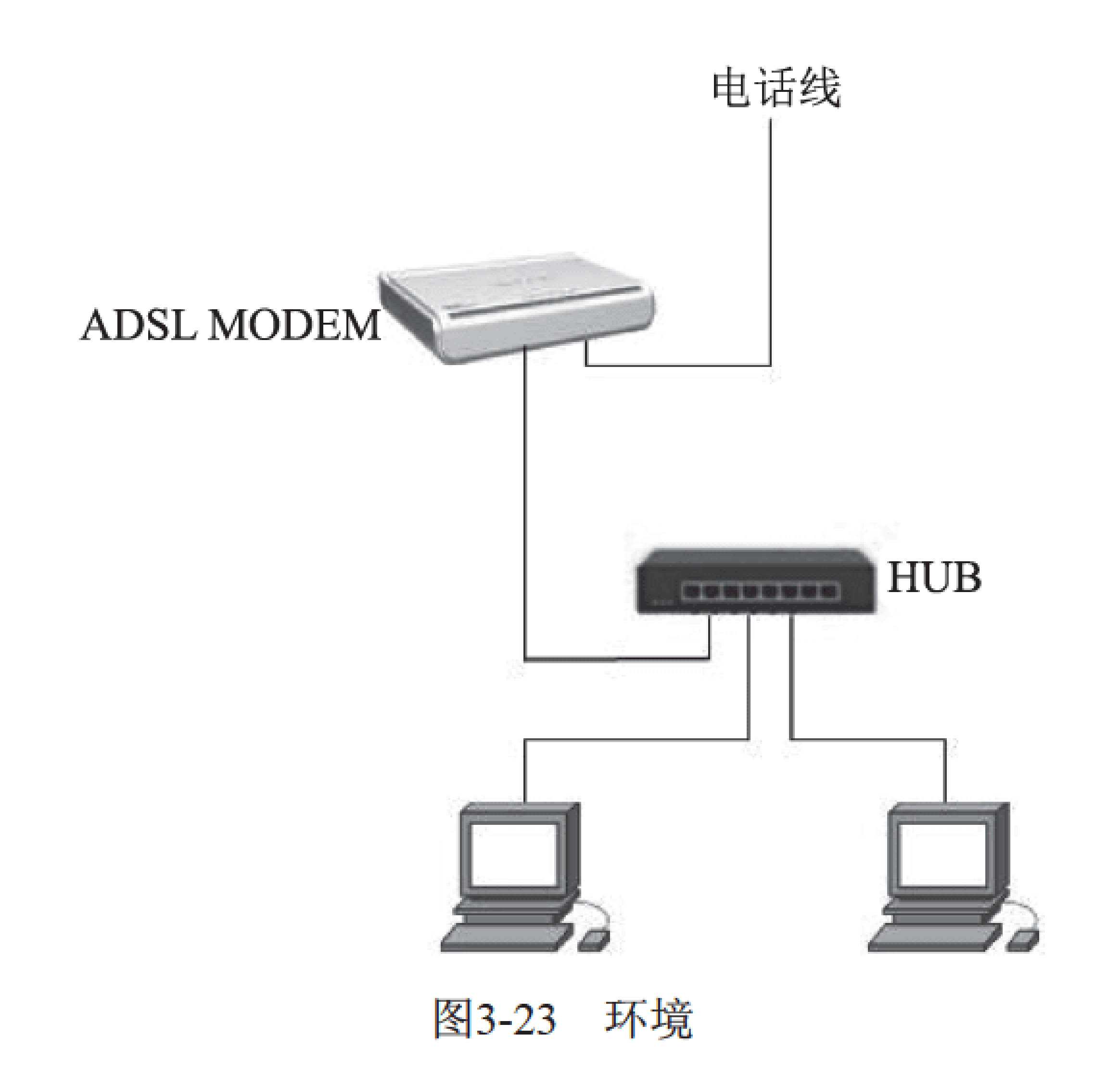


图3-23　环境

但是连好后，在原来电脑上"控制面板"中的"网络连接"，双击"宽带连接"后，输入正确的用户名和密码，点连接后，电脑可以正常访问互联网，但是

另外一台电脑却不能正常访问。

后来我查了些资料，才知道上面这种配置模式上网使用的是ADSL Modem的“桥接”模式，如图3-24所示。这种模式只能保证一台电脑访问互联网，而且每次上网前都要双击“宽带连接”，连接后才能上网。

WAN配置

PVC	0
VPI	0
VCI	35
启用	Yes
模式	桥接
协议	RFC2684
封装格式	LLC

图3-24　“桥接”模式

要想让两台电脑都能访问互联网，可以把ADSL Modem设置成路由模式，如图3-25所示。现在大多数的ADSL Modem都有路由模式功能，一般默认情况下，在连接ADSL Modem的电脑浏览器地址栏中输入http://192.168.1.1后就能进入ADSL Modem的WEB界面控制台，进行相应的设置。填上正确的用户名和密码后点保存即可。

WAN配置

PVC	0
VPI	0
VCI	35
启用	Yes
模式	路由
协议	PPPoE
封装格式	LLC
登录信息	
服务商名称	ISP123
用户名	huawei123
密码	••••••
PPP认证	AUTO

图3-25　WAN配置

使用路由模式还有一个好处就是，每次开机上网，不用再双击“宽带连接”进行连接了，只要开机后电脑会自动进行连接，包括电脑IP地址、DNS服务器地址等都是自动获取。不过若ADSL不是包月的用户，要注意不上网时关闭ADSL Modem，以避免不必要的费用。

3.8　运维实例：巧妙利用双绞线中闲置的数据线

公司因工作需要，新聘用了一名工作人员，我负责为其搭建能访问Internet的网络连接。经过测试他房间中的信息插座和机房配线架之间的双绞线中，第1、2根数据线故障，不能传输数据，正好影响到双绞线中用来传输数据的第1、2、3、6根中的两根。

刚开始想到用一个具有5端口的D-Link小交换机进行连线，因房间中还有一位工作人员通过另外一个信息插座，能正常访问Internet。用一根网线连接D-Link交换机和房间中正常的信息插座，然后再用两根网线分别连接房间内两位工作人员的电脑和D-Link交换机即可。

但后来突然想到，双绞线中第4、5、7、8根是闲置的，何不利用闲置中的两根来代替故障的第1、2根数据线来传输数据，所以就有了如图3-26所示的方案。

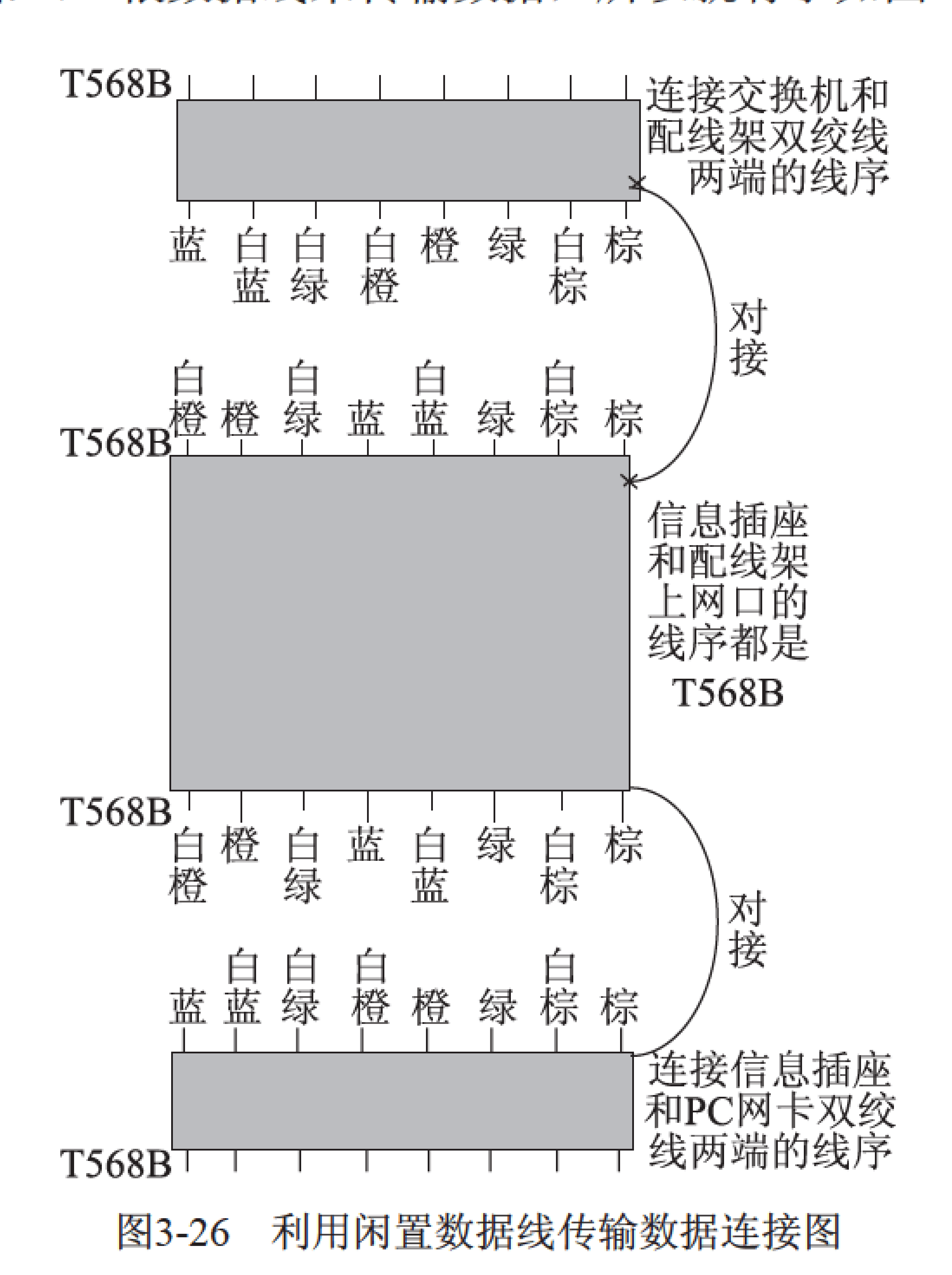


图3-26　利用闲置数据线传输数据连接图

图3-26所示方案其实就是用配线架和信息插座网口之间闲置的第4、5根数据线，

传递已故障的第1、2根数据线中原有的数据，从而避免再使用一D-Link交换机。

安全无小事，对于计算机网络更是这样，网络安全有问题，基础的网络设施建设的再好，可能都会引起致命的问题。网络安全问题，主要包括防火墙、UTM、SSL VPN和入侵检测等设备。不同的安全设备，用途也完全不一样。防火墙是最普遍、也是最常见的安全设备，他的功能就和家里院墙的功能类似，院墙可以把强盗、小偷等坏人拒之墙外。同理，防火墙也可以把互联网上大部分的安全威胁拒之“网”外。

目前，普通的防火墙，主要是针对网络IP地址和端口号做的安全防护。用户在互联网上访问本单位内部的应用系统肯定会经过防火墙设备，而且他访问内部的应用系统，肯定是访问应用系统对应的IP地址和端口号，只要在防火墙上添加策略，只允许用户能访问此应用系统的IP地址和端口，对访问其他的应用的IP和端口，一概拒绝通过。这就好比有许多人想到你家里去，但只允许到你家里找特定的人，并说特定的事的人才能进你家门，这里你要找的那个特定的人就相当于IP地址，特定的事就相当于端口号，并不是说所有想进你家门的人他就能进的，这也就是普通防火墙的作用。

SSL VPN就相当于给互联网上的用户提供了一个访问单位内部应用系统的安全通道，只要你的电脑能上互联网，你有访问单位内部应用系统的权限，使用SSL VPN你就能够实现和在单位内部访问应用系统同样的体验，这也就是SSL VPN的魅力所在，它大大扩展了远程办公应用范围，只要有互联网，在家使用SSL VPN办公和在单位办公体验几乎一样。目前，SSL VPN的使用已经非常普遍，尤其是在网上银行、手机银行和互联网金融方面，更是无所不在。

IDS和IPS也是最常见的网络安全设备，所不同的是前者只有报警提醒功能，不具备执行和截断功能，而后者报警和执行功能都具备。比如说IDS发现有入侵行为，它只能把入侵的情况报告给网络运维人员，至于怎么处理入侵，IDS是无能为力的。而IPS不但能发现，还能够对入侵采取措施，这是IDS所不具备的。另外，在部署上二者也有所不同，IDS一般是连接在交换机的镜像口上，而IPS是绝对不能部署在镜像口上的，要不然IPS的功能就会大打折扣，因为镜像口上是不能有执行和操作功能的，它只是把镜像口上的数据复制到安全设备上，供安全设备分析研究，除此别无其他功能。网络安全设备具体的用途和使用方法，请看官接着往下阅读。

第4章 网络安全

4.1 运维实例：网络安全设备的3种管理模式

目前，随着互联网的高速发展，网络已深入到人们生活的各个方面。网络带给人们诸多好处的同时，也带来了很多隐患。其中，安全问题就是最突出的一个。但是许多信息管理者和信息用户对网络安全认识不足，对网络上的攻击和防护知识缺乏足够的认识和了解，他们把大量的时间和精力用于提升网络的性能和效率方面，结果导致黑客攻击、恶意代码、邮件炸弹等越来越多的安全威胁。

为了防范各种各样的安全问题，许多网络安全产品也相继在网络中得到推广和应用。针对系统和软件的漏洞，有漏洞扫描产品；为了让因特网上的用户能安全、便捷地访问公司的内部网络，就有了SSL VPN和IPSec VPN的使用；为了防止黑客的攻击入侵，就有了入侵防御系统和入侵检测系统；而使用范围最为广泛的防火墙，常常是作为网络安全屏障的第一道防线。网络中安全设备使用的增多，相应地在设备的管理上就日益复杂。下面就通过一则实例，并结合网络的规模和复杂程度，详细阐述网络中安全设备管理的3种模式。

1. 公司网络架构

1)总架构

网络结构图如图4-1所示。为了确保重要设备的稳定性和冗余性，核心层交换机使用两台Cisco4510R，通过Trunk线连接。在接入层使用了多台Cisco3560-E交换机，图示为了简洁，只画出了两台。在核心交换机上连接有单位重要的服务器，如DHCP、E-MAIL服务器、WEB服务器和视频服务器等。单位IP地址的部署，使用的是C类私有192网段的地址。其中，DHCP服务器的地址为192.168.11.1/24。在网络的核心区域部署有单位的安全设备，安全设备也都是通过Cisco3560-E交换机接入到核心交换机4510R上，图4-1中为了简洁，没有画出3560-E交换机。

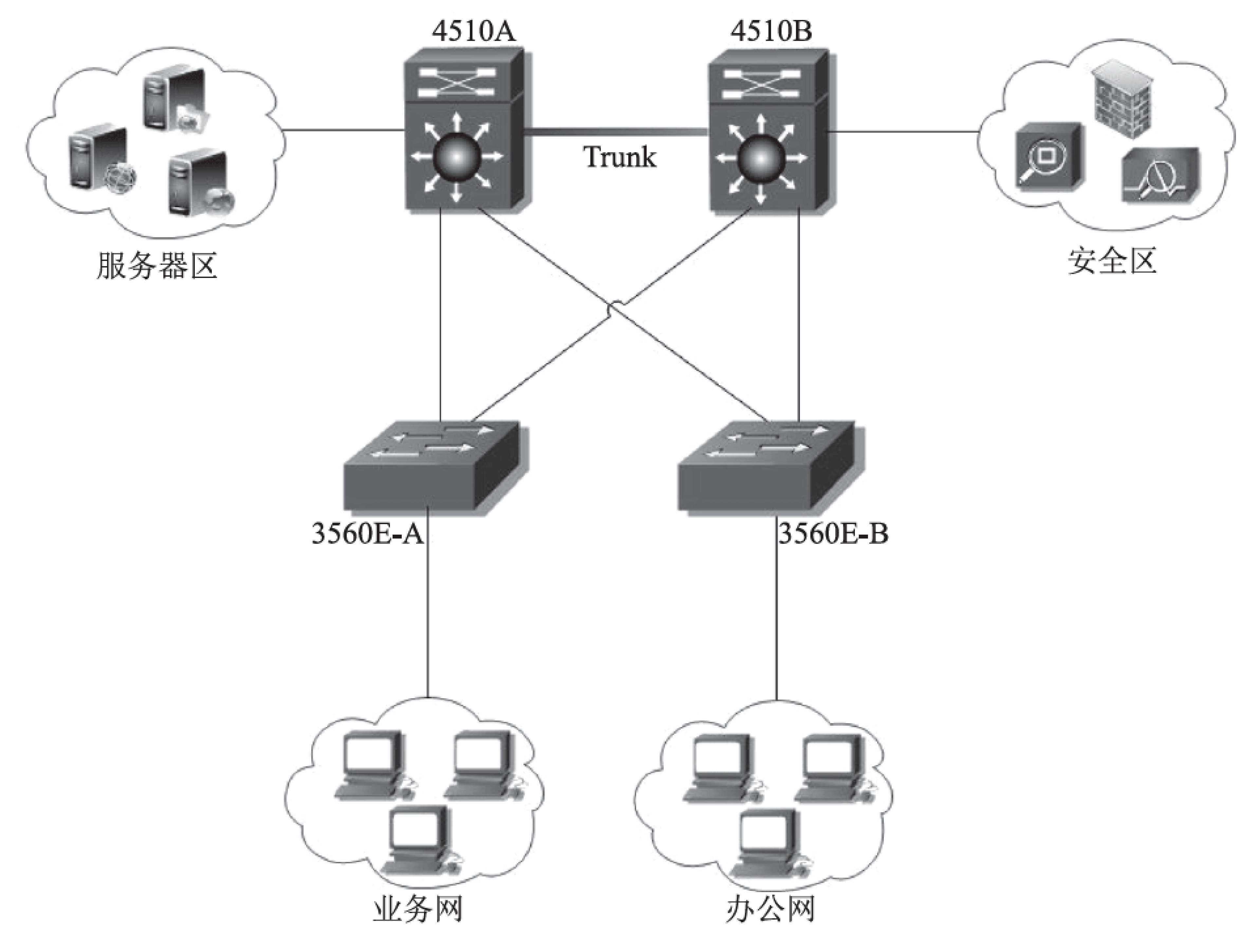


图4-1　网络结构图

2)主要网络设备配置

网络主要分为业务网和办公网，业务网所使用VLAN的范围是VLAN 21～VLAN 100，办公网所使用的VLAN范围是VLAN 101～VLAN 200。两个网都是通过两台核心交换机4510交换数据的，但在逻辑上是相互隔离的。服务器都是直接连接到4510上，所使用的VLAN范围是VLAN 11～VLAN 20。安全设备所使用的VLAN范围是VLAN 2～VLAN 10。

(1)在业务网中，根据部门性质的不同，在Cisco4510和Cisco3560上做相应的配置，把它们划分到不同的VLAN中。下面以业务网中VLAN 21的配置为例，列出其相关命令，首先是在Cisco3560E-A上的配置如下所示：

```
Cisco3560E-A#vlan database
Cisco3560E-A(VLAN)#VLAN 21          //创建VLAN 21
VLAN 21 added:
```

```
Name: VLAN00021
Cisco3560E-A(VLAN)#exit
Cisco3560E-A# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Cisco3560E-A (config)#interface range gigabitEthernet 1/0/1-24
//对3560上1至24端口同时进行配置
Cisco3560E-A (config-if-range)# switchport
Cisco3560E-A (config-if-range)#switchport access VLAN 21
//把3560上1至24端口都划入VLAN 21
```

Cisco4510A上的配置如下所示：

```
Cisco4510A(config)#interface VLAN 21
Cisco4510A(config-if)#ip address 192.168.21.252 255.255.255.0
//创建VLAN 21的SVI接口，并指定IP地址
Cisco4510A(config-if)#no shutdown
Cisco4510A(config-if)ip helper-address 192.168.11.1
//配置DHCP中继功能
Cisco4510A(config-if)standby 21 priority 150 preempt
Cisco4510A(config-if)standby 21 ip 192.168.21.254
//配置VLAN 21的HSRP参数
```

(2)同样在办公网中，也是根据部门性质的不同，把它们划分到不同的VLAN中，下面是办公网中VLAN 101的配置，首先是在Cisco3560E-B上的配置如下所示：

```
Cisco3560E-B#vlan database
Cisco3560E-B(VLAN)#VLAN 101          //创建VLAN 101
VLAN 101 added:
Name: VLAN000101
Cisco3560E-B(VLAN)#exit
Cisco3560E-B# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Cisco3560E-B (config)#interface range gigabitEthernet 1/0/1-24
//对3560上1至24端口同时进行配置
Cisco3560E-B (config-if-range)# switchport
Cisco3560E-B (config-if-range)#switchport access VLAN 101
//把3560上1至24端口都划入VLAN 101
```

Cisco4510B上的配置如下所示：

```
Cisco4510B(config)#interface VLAN 101
Cisco4510B(config-if)#ip address 192.168.101.252 255.255.255.0
//创建VLAN 101的SVI接口，并指定IP地址
Cisco4510B(config-if)#no shutdown
Cisco4510B(config-if)ip helper-address 192.168.11.1
//配置DHCP中继功能
Cisco4510B(config-if)standby 101 priority 150 preempt
Cisco4510B(config-if)standby 101 ip 192.168.101.254
//配置VLAN 101的HSRP参数
```

2. 网络安全设备管理的三种模式

1)第一种模式：安全管理PC直接与安全设备进行连接

如图4-2所示，网络中共有4台安全设备：漏洞扫描、IDS、IPS和防火墙，若要对其中的一台安全设备进行管理配置，就得把电脑直接连接到安全设备上，这种模式通常有以下两种连接管理方式：

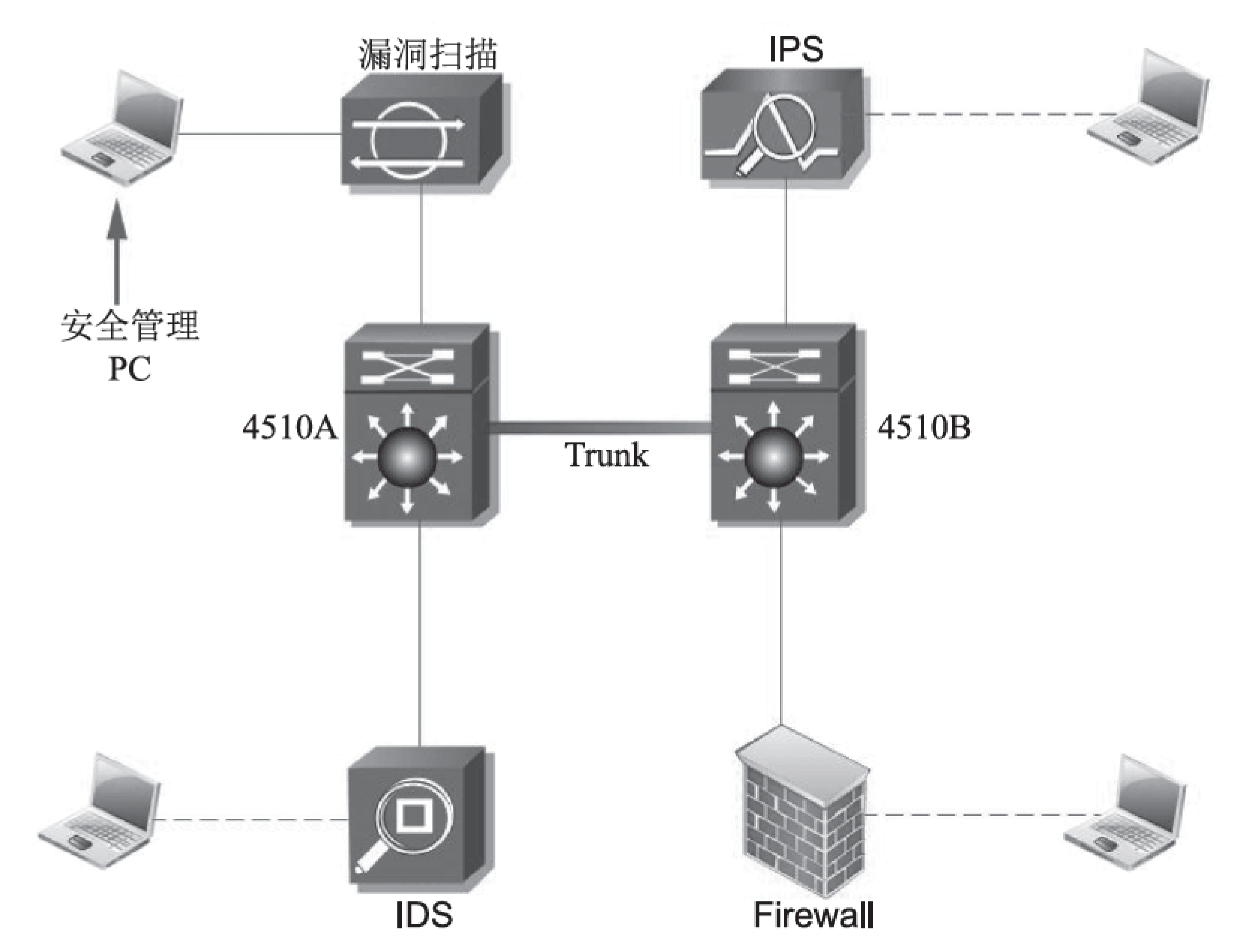


图4-2　安全管理PC和安全设备直接相连

(1)串口连接管理。通过CONSOLE口直接连接到安全设备上，对其进行本地管理配置。这也是一种安全、可靠的配置维护方式。当安全设备初次上电、与外部网络连接中断或出现其他异常情况时，通常采用这种方式配置安全设备。配置步骤如下：

将安全管理PC的串口与安全设备的CONSOLE口连接，然后在PC 机上运行终端仿真程序，如Windows系统中的超级终端，或者使用SecureCRT应用程序。然后在终端仿真程序上建立新连接。

选择实际连接安全设备时，使用的安全管理PC上的串口，配置终端通信参数，默认情况下都是：9600 波特、8 位数据位、1 位停止位、无校验、无流控。

对安全设备进行上电自检，系统自动进行配置，自检结束后提示用户键入回车，直到出现命令行提示符。然后就可键入命令，配置安全设备，或者查看其运

行状态。

上面连接方式中的配置参数，是一般情况下使用较多的一种，但对于不同设备可能会有不同的设置，例如对于防火墙，联想的连接参数就和上面不一致，如图4-3所示。

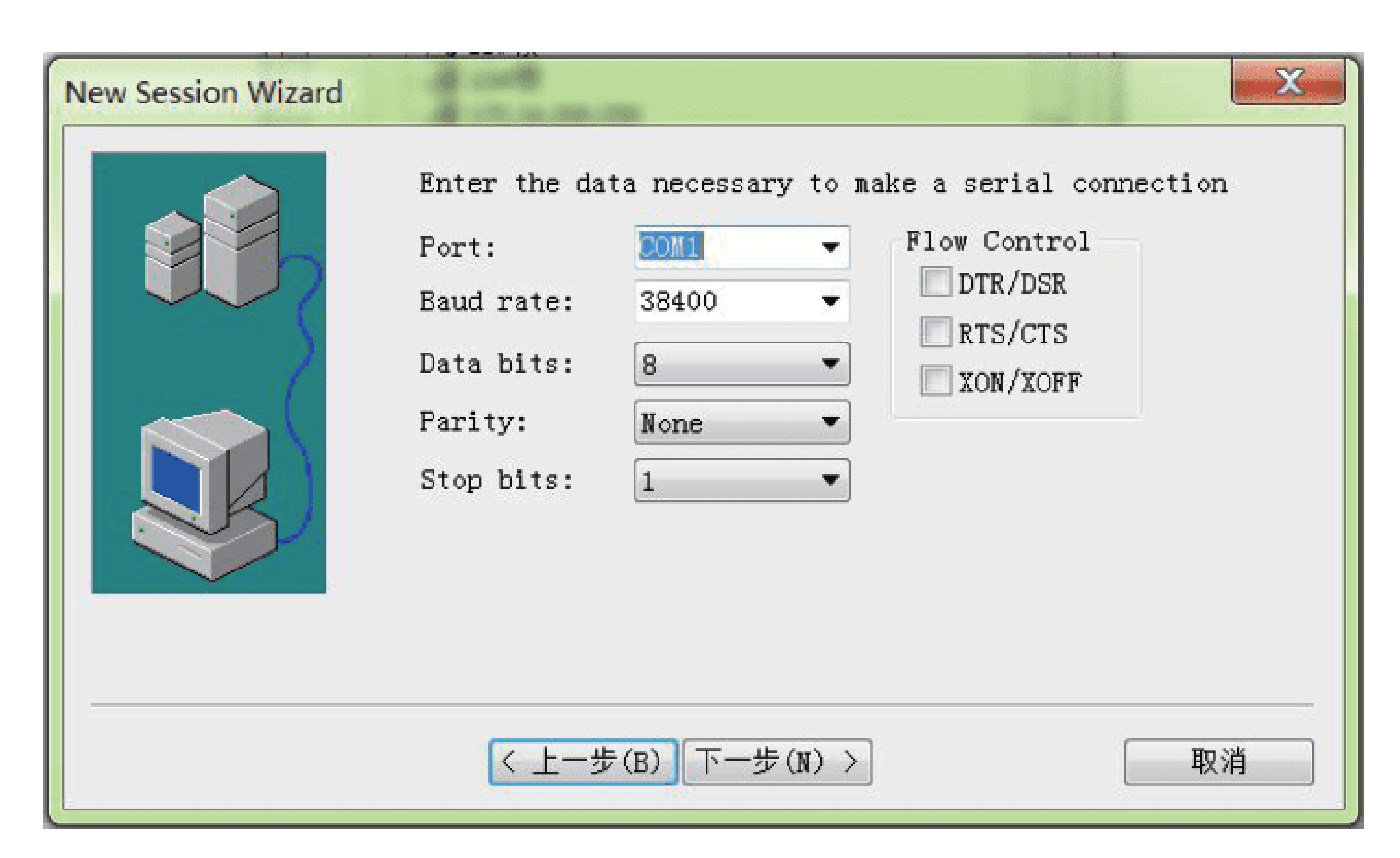


图4-3　终端仿真程序连接安全设备的参数设定

波特率必须选择38400，而且不能选择“RTS/CTS”。其他的参数都和上面的一致。这就要求用这种方式管理配置安全设备时，必须认真查看产品的说明书，不能在终端仿真程序上对所有的参数都使用默认的配置。

(2)WEB方式管理。用这种方式对网络安全设备进行管理，全都是以窗口界面操作的，比较容易理解和掌握。配置的步骤如下：

用网线把安全管理PC的网卡接口，直接连到安全设备的管理接口上。同时，也要对安全管理PC和安全设备的管理接口的IP地址进行配置，以便让它们位于同一个网段。假如配置安全管理PC的IP地址是192.168.1.2/24，安全设备管理接口的IP地址是192.168.1.1/24，这样配置后它们就都位于同一个网段192.168.1.0/24中。

在安全管理PC的“命令行”中，执行命令“ping 192.168.1.1”，看是否能ping通，若不通的话，可能是连接安全管理PC和安全设备的网线有故障，直到能ping通为止。

开启安全设备的本地SSH 服务，并且允许管理账号使用SSH。这是因为对大多数安全设备的WEB管理都是通过SSH连接设备的，这样安全管理PC和安全设

备之间传输的数据都是通过加密的，安全性比较高。也就是在安全管理PC的浏览器地址栏中只能输入以“https”开头的网址。

在安全管理PC的浏览器地址栏中输入“https://192.168.1.1”回车，输入用户名和密码后就可登录到网络安全设备的WEB管理界面，对其参数和性能进行配置。

2)第二种模式：安全管理PC通过交换机管理安全设备

如图4-4所示，安全设备位于VLAN 2、VLAN 3和VLAN 4中。这时，安全管理PC对位于同一个VLAN中的安全设备进行管理时，只需把安全管理PC直接连接到交换机上，PC和安全设备就都位于同一网段中。在这种模式中，对安全设备的管理，就不能使用“第一种模式”中的用CONSOLE口管理的方法，因为安全管理PC和安全设备没有直接连接，而是通过交换机间接连接起来的。这种模式下，除了可以用“第一种模式”中的WEB方式对安全设备进行管理配置外，还可以用以下两种方式对安全设备进行管理配置：

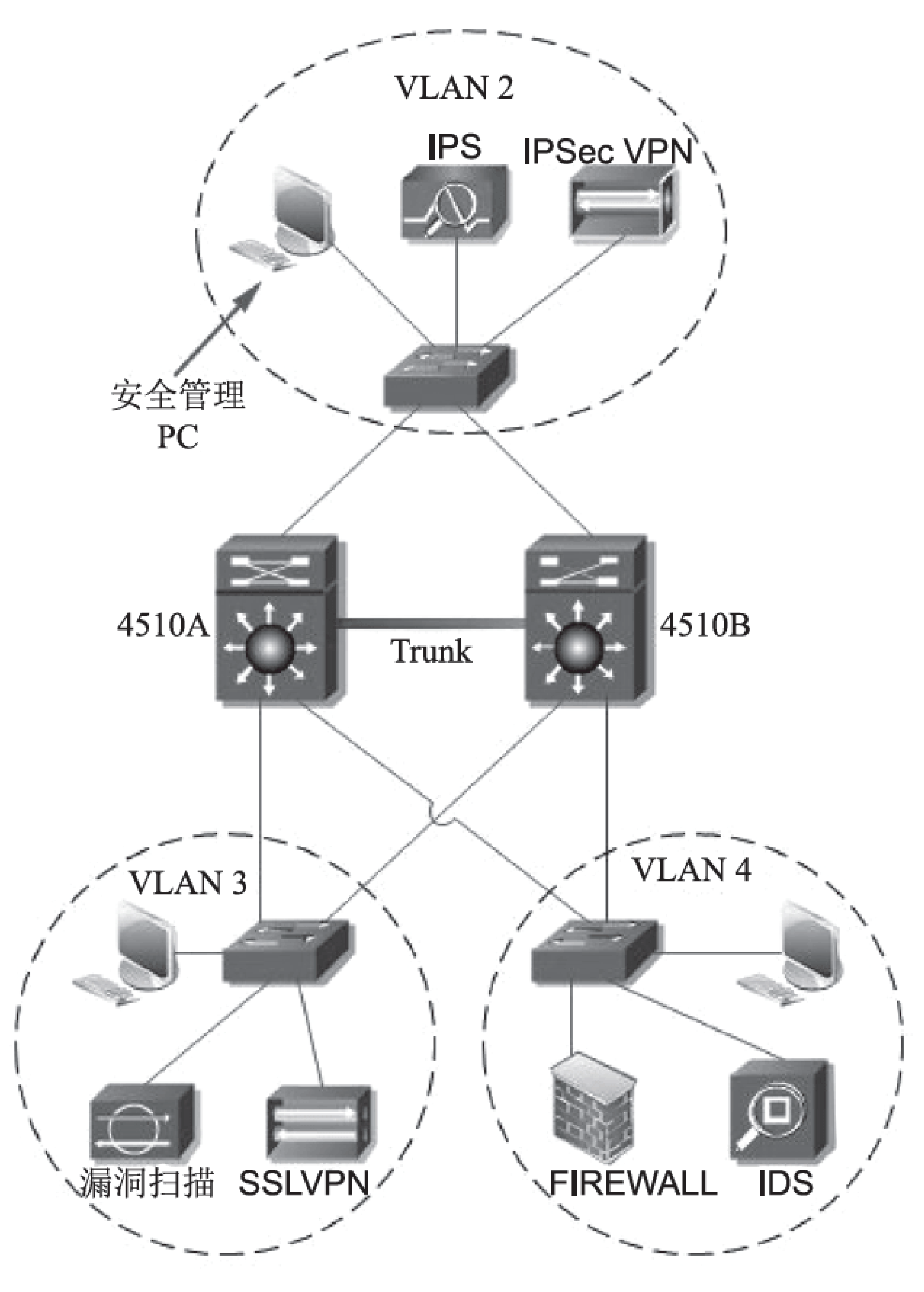


图4-4　管理PC通过交换机连接到安全设备

(1)Telnet方式管理。用这种方式对安全设备进行管理时，必须首先保证安全管理PC和安全设备之间有路由可达，并且可以用Telnet 方式登录到安全设备上。在本例中，安全管理PC和安全设备位于同一个网段，所以满足用Telnet方式管理的条件。另外，还要在安全设备上进行如下配置，才能采用Telnet 方式对其进行管理。

把一台电脑的串口连接到安全设备的CONSOLE口上。通过CONSOLE口配置远程用户用Telnet方式登录到安全设备上的用户名和口令、管理级别及所属服务等。

通过CONSOLE口配置提供Telnet 服务的IP地址、端口号等。

在安全管理PC上的“命令行”中，执行Telnet到网络安全设备上的命令，然后输入用户名和口令，就可以登录到安全设备上进行管理配置了。

(2)SSH方式管理。当用户在一个不能保证安全的网络环境中时，却要远程登录到安全设备上。这时，SSH 特性就可以提供安全的信息保障及认证功能，起到保护安全设备不受诸如IP 地址欺诈、明文密码截取等攻击。安全管理PC以SSH方式登录到安全设备之前，通常还要在安全设备上进行如下配置：

通过一台电脑连接到安全设备的CONSOLE口，或者通过WEB管理方式，登录到安全设备上。

在安全设备上配置SSH服务器的参数，如验证方式、验证重复的次数和兼容的SSH版本等。

在安全管理PC上运行SSH的终端软件，如SecureCRT应用程序。在程序中设置正确的连接参数，输入安全设备接口的IP 地址，就可与安全设备建立起连接，然后对其进行配置管理。

3)第三种模式：通过安全中心服务器管理安全设备

如图4-5所示，与第一、二种管理模式相比，此种模式把“安全管理PC”升级成了“安全中心服务器”。在服务器上就可以对网络中所有的安全设备进行管理配置，而不用再把安全管理PC逐个地连接到安全设备或安全设备所在VLAN的交换机上。在这种管理模式中，除了不能直接连接到安全设备的CONSOLE口上对其进行管理配置外，其他的三种管理方式，WEB、Telnet和SSH在安全中心服务器上都可以使用。用安全中心服务器管理配置安全设备主要存在两种网络环境：

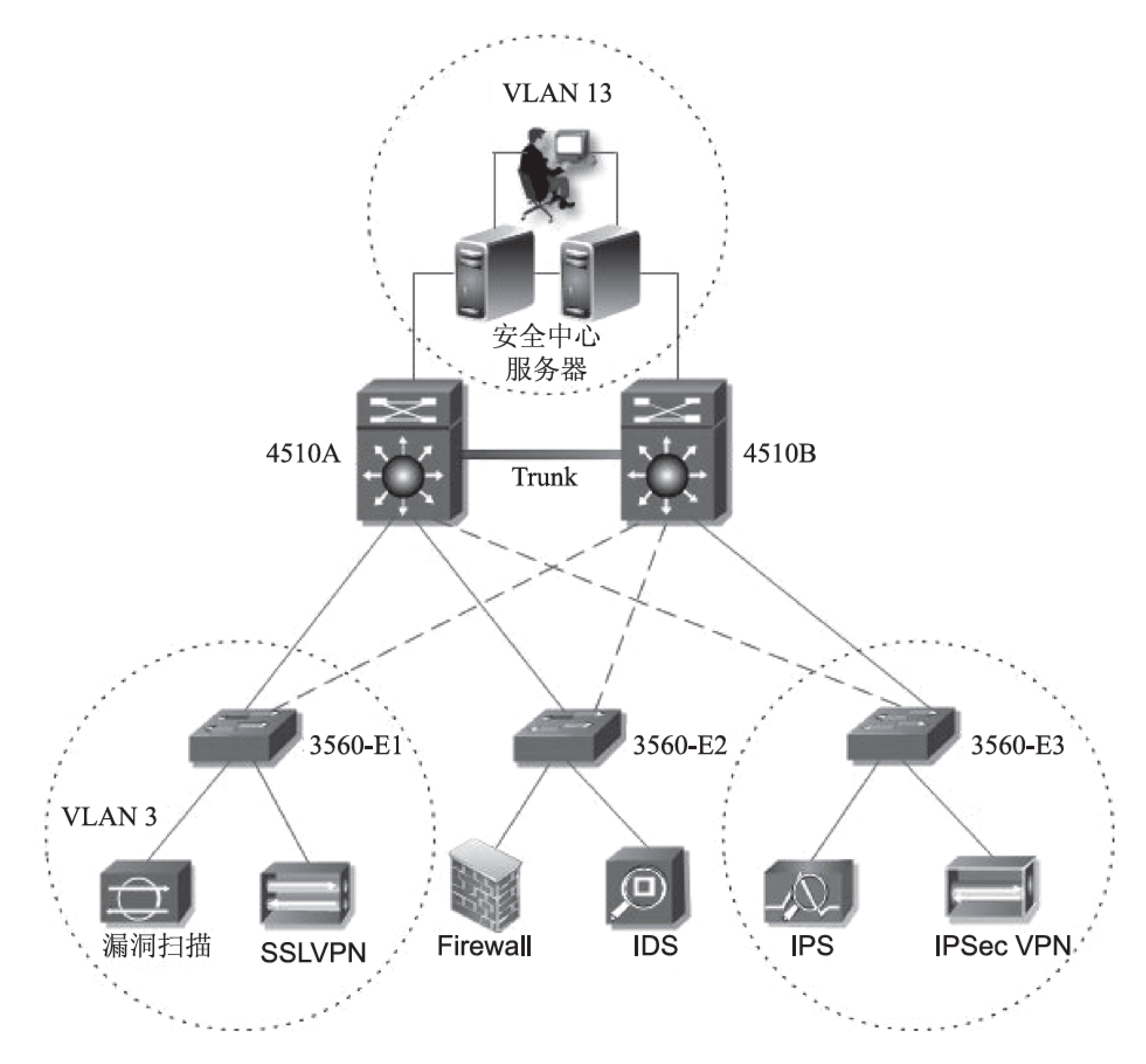


图4-5 通过安全中心服务器管理安全设备

(1)安全中心服务器和安全设备管理接口的IP地址不在同一个网段。如图4-5所示，安全中心服务器位于VLAN 13，IP地址为192.168.13.1/24。而漏洞扫描位于VLAN 3中，IP地址为192.168.3.1，它和安全服务中心服务器的地址位于不同的子网中。如果要让安全服务中心服务器能访问到漏洞扫描，就必须在两台Cisco4510上添加三层配置，让两个VLAN间的数据能互相访问。在4510A和4510B上的配置如下所示：

Cisco4510A上的配置如下所示：

```
Cisco4510A(config)#interface VLAN 13
Cisco4510A(config-if)#ip address 192.168.13.252 255.255.255.0
```

```
//创建VLAN 13的SVI接口，并指定IP地址
Cisco4510A(config-if)#no shutdown
Cisco4510A(config-if)ip helper-address 192.168.11.1
//配置DHCP中继功能
Cisco4510A(config-if)standby 13 priority 150 preempt
Cisco4510A(config-if)standby 13 ip 192.168.13.254
//配置VLAN 13的HSRP参数

Cisco4510A(config)#interface VLAN 3
Cisco4510A(config-if)#ip address 192.168.3.252 255.255.255.0
//创建VLAN 3的SVI接口，并指定IP地址
Cisco4510A(config-if)#no shutdown
Cisco4510A(config-if)ip helper-address 192.168.11.1
//配置DHCP中继功能
Cisco4510A(config-if)standby 3 priority 150 preempt
Cisco4510A(config-if)standby 3 ip 192.168.3.254
//配置VLAN 3的HSRP参数
```

Cisco4510B上的配置如下所示：

```
Cisco4510B(config)#interface VLAN 13
Cisco4510B(config-if)#ip address 192.168.13.253 255.255.255.0
//创建VLAN 13的SVI接口，并指定IP地址
Cisco4510B(config-if)#no shutdown
```

```
Cisco4510B(config-if)ip helper-address 192.168.11.1
//配置DHCP中继功能
Cisco4510B(config-if)standby 13 priority 140 preempt
Cisco4510B(config-if)standby 13 ip 192.168.13.254
//配置VLAN 13的HSRP参数


Cisco4510B(config)#interface VLAN 3
Cisco4510B(config-if)#ip address 192.168.3.253 255.255.255.0
//创建VLAN 3的SVI接口，并指定IP地址
Cisco4510B(config-if)#no shutdown
Cisco4510B(config-if)ip helper-address 192.168.11.1
//配置DHCP中继功能
Cisco4510B(config-if)standby 3 priority 140 preempt
Cisco4510B(config-if)standby 3 ip 192.168.3.254
//配置VLAN 3的HSRP参数
```

因为4510和3560-E之间都是Trunk连接，所以在4510A和4510B上进行了如上配置后，安全中心服务器就能访问到漏洞扫描安全设备。在安全中心服务器的浏览器地址栏中输入https://192.168.3.1，就能登录到漏洞扫描设备上，然后在WEB界面中就可以对其参数和性能进行配置。

(2)安全中心服务器和安全设备管理接口的IP地址都位于同一个网段中。这种网络环境中，安全中心服务器要对安全设备进行管理时，在路由器或交换机上需要配置的命令就比较少。也就是在图4-5中，只需把交换机上的配置命令进行简单的改造，把所有的安全设备的管理接口的IP地址和安全中心服务器地址配置到同一个VLAN中。这样在Cisco4510上就不用进行三层配置。然后在安全中心服务器的浏览器地址栏中输入安全设备的IP地址也能对各个安全设备进行管理配置。

3. 总结

(1)以上3种网络安全设备的管理模式，主要是根据网络的规模和安全设备的多少，来决定使用哪一种管理模式。3种模式之间没有完全的优劣之分。若是网络中就一两台安全设备，显然采用第一种模式比较好。只需要一台安全管理PC就可以。若是采用架设安全中心服务器的话就有些得不偿失。如果安全设备较多，并且都分布在不同的网段，那选择第二种模式就行，用两三台安全管理PC管理安全设备，比架设两台服务器还是要经济很多。若是安全设备很多，就采用第3种模式，它至少能给网络管理员节省很多的时间，因为在一台服务器上就它就可以对所有的安全设备进行管理。

(2)第三种管理模式中，安全中心服务器共使用了两台服务器。这主要是因为，在一些大型的网络中，安全设备不只是有几台、十几台，有的已达上百台，或者更多。管理这么多数量的安全设备，完全有必要架设两台服务器，保证管理安全设备的稳定性和可靠性。而且，安全中心服务器有时并不仅仅承担着管理的功能，它有时还要提供安全设备软件的升级功能。也就是在安全中心服务器上提供一个访问Internet的接口，所有的安全设备都通过这个接口连接到互联网上进行升级，例如防火墙系统版本、病毒特征库的升级，IPS系统版本和特征值的升级等。若安全设备很多，升级数据量就会很大，若用两台服务器双机均衡负载，会大大降低用一台服务器升级时所面临巨大数据量的压力。

(3)解决网络安全问题主要是利用网络管理措施，保证网络环境中数据的机密性、完整性和可用性。确保经过网络传送的信息，在到达目的地时没有任何增加、改变、丢失或被非法读取。而且要从以前单纯的以防、堵、隔为主，发展到现在的攻、防结合，注重动态安全。在网络安全技术的应用上，要注意从正面防御的角度出发，控制好信息通信中数据的加密、数字签名和认证、授权、访问等。而从反面要做好漏洞扫描评估、入侵检测、病毒防御、安全报警响应等。要对网络安全有一个全面的了解，不仅需要掌握防护方面的知识，也需要掌握检测和响应环节方面的知识。

互联网上发生的大大小小的泄密事件，也再次给我们敲响了警钟，网络安全无小事，网络安全管理也必须从内、外两方面来防范。计算机网络最大的不安全，就是自认为网络是安全的。在安全策略的制定、安全技术的采用和安全保障的获得，其实很大程度上要取决于网络管理员对安全威胁的把握。网络上的威胁

时刻存在，各种各样的安全问题常常会掩盖在平静的表面之下，所以网络安全管理员必须时刻提高警惕，把好网络安全的每一道关卡。

4.2 运维实例：防火墙部署搭建与故障排除

安全无小事！互联网上的每一次“密码泄露”事件都闹得沸沸扬扬，人心惶惶。例如，CSDN用户数据库的泄露事件，对从事计算机技术工作的人是当头一棒。因为IT技术工作者，绝大多数都在CSDN注册过账号，而且几乎都是使用同一个用户名和密码注册了其他类的技术网站。发生“CSDN用户数据库泄露”事件后，反正我是赶紧把自己在用的许多技术类网站的密码都改了过来。但是刚改完没多久，又出现了天涯、新浪微博等泄密事件。真是防不胜防！

难道互联网上就没有安全的地方了吗？我认为还是有的，要不然也没有这么多人使用互联网。只不过近段时间暴露的问题接二连三，太多了。不过，有了问题只要通过各种安全措施把它解决了，同样可以提高互联网的安全性。所以，这就对负责IT安全的技术人员有了更高的要求。本篇文章就涉及到企业网中防火墙设备部署、安装和配置。虽然防火墙不能解决所有的安全问题，但它在网络中的部署也是绝对不能少的。

1. 网络架构和防火墙部署情况

网络结构图如图4-6所示。为了确保重要设备的稳定性和冗余性，核心层交换机使用两台6509-E，通过Trunk线连接。在办公区的接入层使用了多台Cisco2960交换机，图示为了简洁，只画出了两台。在核心层交换机6509-E上，通过防火墙连接有单位重要的服务器，如FTP、E-MAIL服务器和数据库等。单位IP地址的部署，使用的是C类私有192网段的地址。DHCP服务器的IP地址为192.168.10.1，FTP服务器的IP地址是192.168.5.2。Cisco6509-E和Cisco3750之间及Cisco3750和Cisco2960之间都是Trunk连接。

图4-6中的黄色线表示的是用光纤连接，蓝色线表示的是用双绞线连接。而且从两台6509上分别延伸出来了的两条黄色线，一条竖线和一条横线，它们在拓扑图中其实是对两台6509上端口的一种扩展，并不是这两条线只连接到6509

上的一个端口，而是连接了多个端口。这种布局的拓扑图，在结构上就显得更清晰明了。

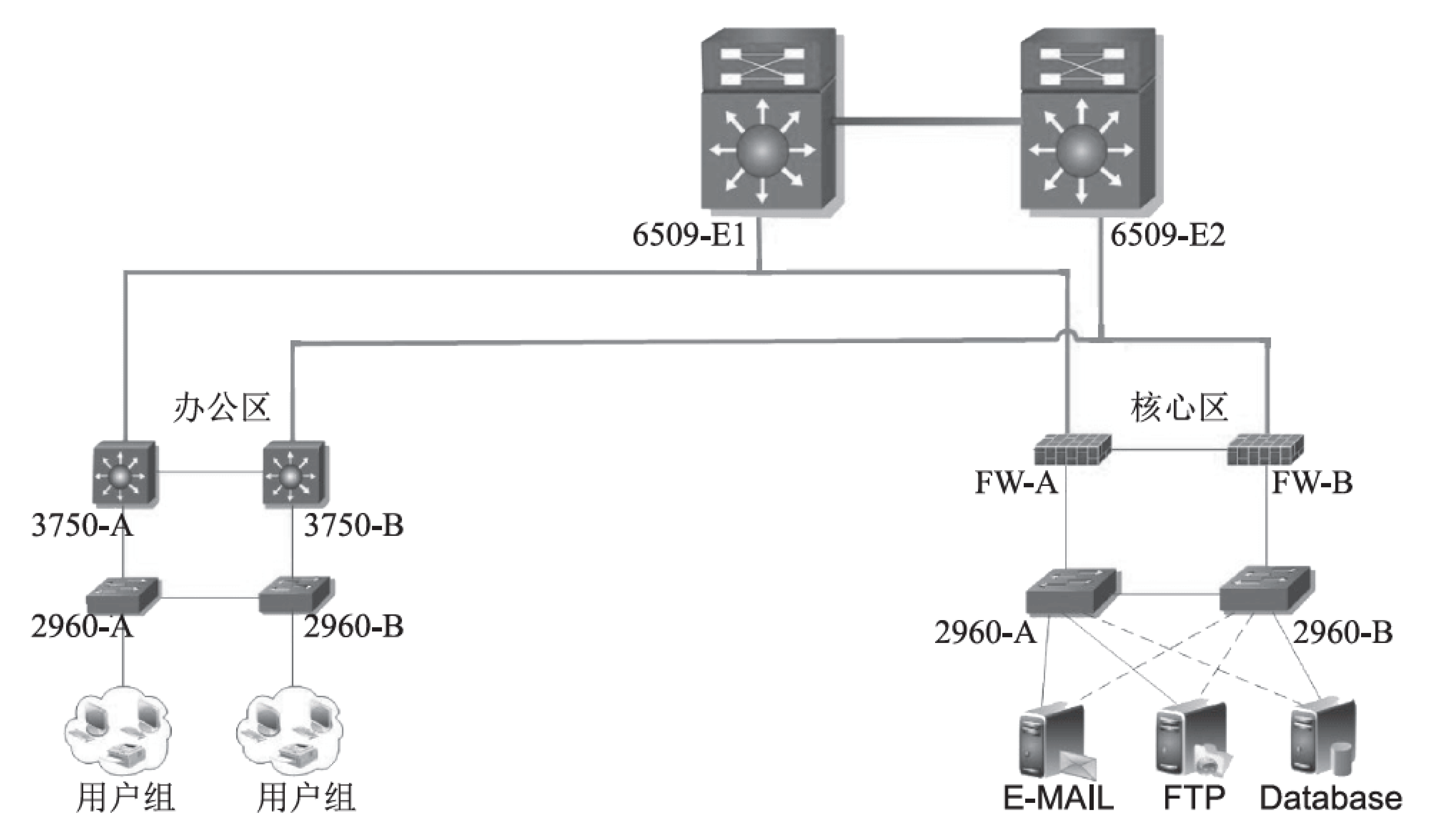


图4-6　网络架构和防火墙部署图示

根据部门性质的不同，把各个部门的电脑划入到不同的VLAN中。服务器都位于VLAN 2～VLAN 10中，对应的网络号是192.168.2.0～192.168.10.0，如DHCP服务器位于VLAN 10中，FTP服务器位于VLAN 5中。服务器的IP地址、默认网关和DNS都是静态配置的。VLAN 11～VLAN 150是属于办公部门使用的，对应的网络号是192.168.11.0～192.168.150.0。VLAN号和网络号之间都是对应的。VLAN中的PC都是通过Cisco2960接入到网络中，3750都是二层配置，三层的配置都在Cisco6509上，也就是VLAN间的路由都是通过6509完成的。PC的IP地址、默认网关和DNS都是自动从DHCP服务器上获得的，不用手工静态配置。

如图4-6所示，两台防火墙都是联想Power V防火墙，它们运行的模式都为透明模式，也就是以“桥”模式运行的，本身只需要配置一个管理IP地址，不必占用任何其他的IP资源，也不需要改变用户的拓扑环境，设备的运行对用户来说是“透明”的，在网络设备上进行各种命令的配置时，就当不存在这两个防火墙一样，因为它们是透明模式。它们只对线路上的数据包作安全检查和安全策略上的限制，本身不会影响网络的整体架构和配置。这种模式在安装和维护防火墙时，相对防火墙的另外一种运行模式——路由模式来说要简单很多。

Cisco6509-E和核心区Cisco2960之间不是Trunk模式连接，而是使用接入模式连接的，也就是两台Cisco6509-E的Gi3/2位于VLAN 5中，核心区两台Cisco2960的Gi0/1也位于VLAN 5中。两台6509和两台3750之间以及办公区中网络设备间的连接情况如下所示：

```
Cisco6509-E1 GigabitEthernet 3/1 <----> Cisco3750A GigabitEthernet 1/0/25
Cisco6509-E2 GigabitEthernet 3/1 <----> Cisco3750B GigabitEthernet 1/0/25
Cisco3750A GigabitEthernet 1/0/1 <-----> Cisco2960A GigabitEthernet 0/1
Cisco3750B GigabitEthernet 1/0/1 <-----> Cisco2960B GigabitEthernet 0/1
```

两台6509和两台防火墙之间的及核心区中网络设备间的连接情况如下所示：

```
Cisco6509-E1 GigabitEthernet 3/2 <---> FW-A GigabitEthernet 1
Cisco6509-E2 GigabitEthernet 3/2 <---> FW-B GigabitEthernet 1
FW-A GigabitEthernet 2 <---> Cisco2960A GigabitEthernet 0/1
FW-B GigabitEthernet 2 <---> Cisco2960B GigabitEthernet 0/1
```

2. 主要网络设备上的配置情况

1)两台核心交换机上的配置情况。在Cisco6509-E1上的主要配置如下所示：

```
hostname Cisco 6509-E1
!
interface GigabitEthernet3/1
```

```
description Link3750A_1/0/25
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 5,115
 switchport mode trunk
!
interface GigabitEthernet3/2
 description Link_FW-A_Gi1
 switchport access VLAN 5
 switchport mode access
!
interface VLAN5
 ip address 192.168.5.252 255.255.255.0
 standby 5 ip 192.168.5.254
 standby 5 priority 120
 standby 5 preempt
!
interface VLAN115
 ip address 192.168.115.252 255.255.255.0
 standby 115 ip 192.168.115.254
 standby 115 priority 120
 standby 115 preempt
```

其中命令“ip address 192.168.5.252 255.255.255.0”是给指定的VLAN配置IP地址。

命令“standby 5 priority 120”中的“priority”是配置HSRP的优先级，5为组序号，它的取值范围为0～255，120为优先级的值，取值范围为0～255，数值越大优先级越高。

优先级将决定一台路由器在HSRP备份组中的状态，优先级最高的路由器将成为活动路由器，其他优先级低的路由器将成为备用路由器。当活动路由器失效后，备用路由器将替代它成为活动路由器。当活动和备用路由器都失效后，其他路由器将参与活动和备用路由器的选举工作。优先级都相同时，接口IP地址高的将成为活动路由器。

“preempt”是配置HSRP为抢占模式。如果需要高优先级的路由器能主动抢占成为活动路由器，则要配置此命令。配置preempt后，能够保证优先级高的路由器失效恢复后总能成为活动路由器。活动路由器失效后，优先级最高的备用路由器将处于活动状态，如果没有使用preempt技术，则当活动路由器恢复后，它只能处于备用状态，先前的备用路由器代替其角色处于活动状态。

命令“standby 5 ip 192.168.5.254”作用是启动HSRP，如果虚拟IP地址不指定，路由器就不会参与备份。虚拟IP应该是接口所在的网段内的地址，不能配置为接口上的IP地址。

在Cisco6509-E2上的主要配置如下所示：

```
hostname Cisco 6509-E2
!
interface GigabitEthernet3/1
description Link3750B_1/0/25
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 5,115
 switchport mode trunk
!
interface GigabitEthernet3/2
```

```
 description Link_FW-B_Gi1
 switchport access VLAN 5
 switchport mode access
!
interface VLAN5
 ip address 192.168.5.253 255.255.255.0
 standby 2 ip 192.168.5.254
 standby 2 priority 120
 standby 2 preempt
!
interface VLAN115
 ip address 192.168.115.253 255.255.255.0
 standby 2 ip 192.168.115.254
 standby 2 priority 120
 standby 2 preempt
```

(2)在办公区两台Cisco3750和两台Cisco2960上的配置情况如下所示。在Cisco3750A上的配置如下所示：

```
hostname Cisco3750A
!
interface GigabitEthernet1/0/25
 description Link6509-E1 3/1
 switchport trunk encapsulation dot1q
```

```
 switchport trunk allowed VLAN 5,115
 switchport mode trunk
!
interface GigabitEthernet1/0/1
 description Link2960A 0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 5,115
 switchport mode trunk
```

在Cisco3750B上的配置如下所示：

```
hostname Cisco3750B
!
interface GigabitEthernet1/0/25
 description Link6509-E2 3/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 5,115
 switchport mode trunk
!
interface GigabitEthernet1/0/1
 description Link2960B 0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 5,115
 switchport mode trunk
```

在Cisco2960A上的配置如下所示：

```
hostname Cisco2960A
!
interface GigabitEthernet0/1
 description Link3750A 1/0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 5,115
 switchport mode trunk
```

在Cisco2960B上的配置如下所示：

```
hostname Cisco2960B
!
interface GigabitEthernet0/1
 description Link3750B 1/0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed VLAN 5,115
 switchport mode trunk
```

(3)在核心区两台Cisco2960上的主要配置情况如下所示。在Cisco2960A上的配置如下所示：

```
hostname Cisco2960A
!
interface GigabitEthernet0/1
```

```
 description Link3750A 1/0/1
switchport access VLAN 5
 switchport mode access
```

在Cisco2960B上的配置如下所示：

```
hostname Cisco2960B
!
interface GigabitEthernet0/1
 description Link3750B 1/0/1
switchport access VLAN 5
 switchport mode access
```

注意：在办公区和核心区中Cisco2960交换机上的配置情况是不一样的，前者交换机上的端口的配置为Trunk模式，而后者的端口模式为Access模式。

3. 故障发生及排查故障的过程

配置完上面的命令后，在办公区用户的电脑上，应该就能访问到核心区服务器上的资源。例如在办公区有一用户PC的IP地址为192.168.115.2，子网掩码为255.255.255.0，默认网关为192.168.115.254。它应该是能访问到核心区的FTP服务器，FTP服务器的IP地址为192.168.5.2，子网掩码也是255.255.255.0，默认网关为192.168.5.254。一般在PC浏览器的地址栏中输入“ftp://192.168.5.2”回车后，就能显示出一个对话框，提示输入用户名和密码，然后就能访问到FTP服务器上的资源。但结果却访问不成功，根本就没有对话框提示输入用户名和密码。

办公区用户PC访问核心区FTP服务器的数据流向如图4-7所示。因为在办公区的两台Cisco3750。和核心区的两台防火墙、两台Cisco2960以及两台核心交换机Cisco6509-E都是双机热备或负载均衡的运行模式，所以数据流向只要通过两台中的任意一台就都是正常的。

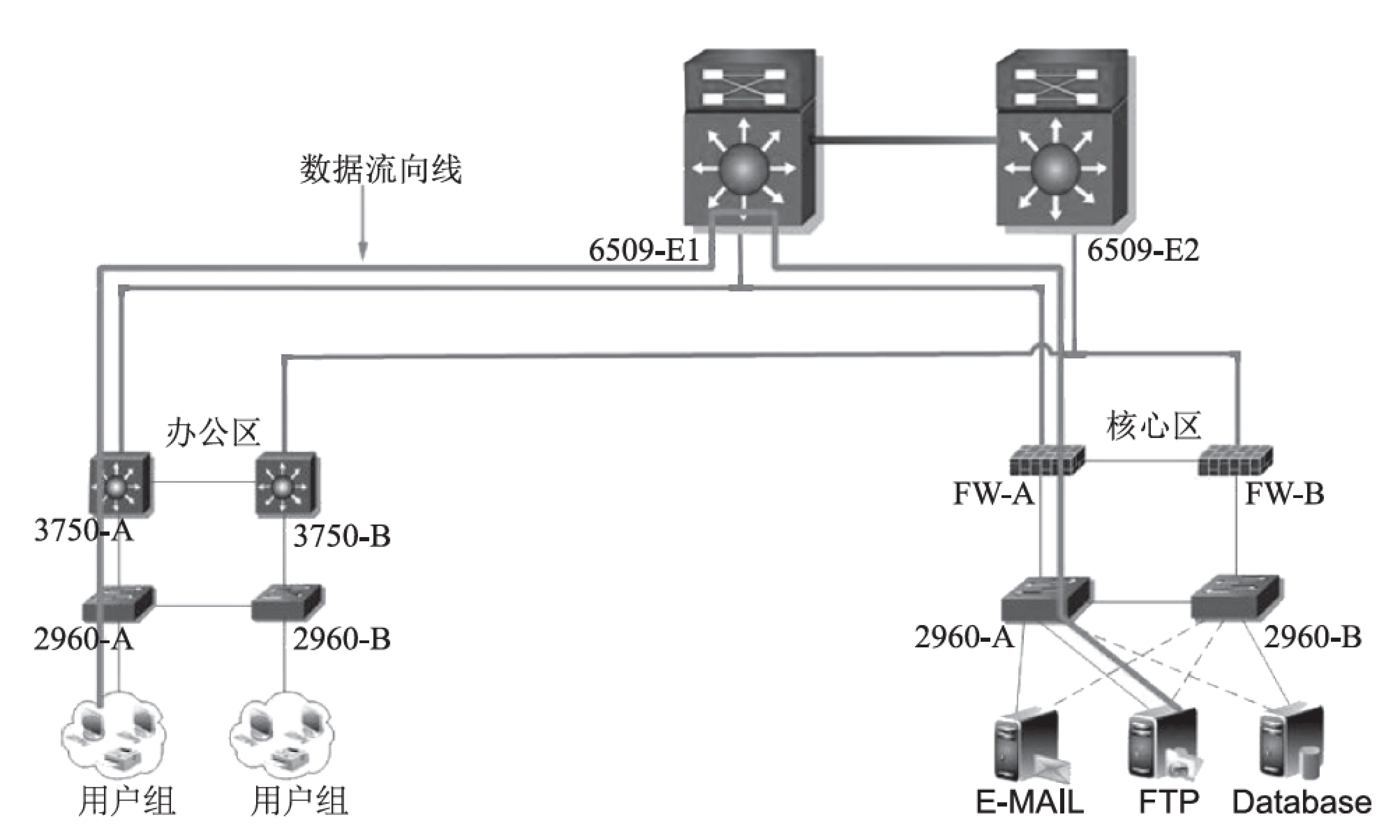


图4-7　办公用户访问FTP服务器的数据流向图示

既然已经知道了数据的流向，也就能大致确定故障发生在什么地方。为了图示的简洁明了，把图4-7再进一步精简，得到如图4-8所示的拓扑图。从图4-8中可以看出，整个的数据流向就一条线，这样排查故障也就比较简单，排查故障的步骤如下：

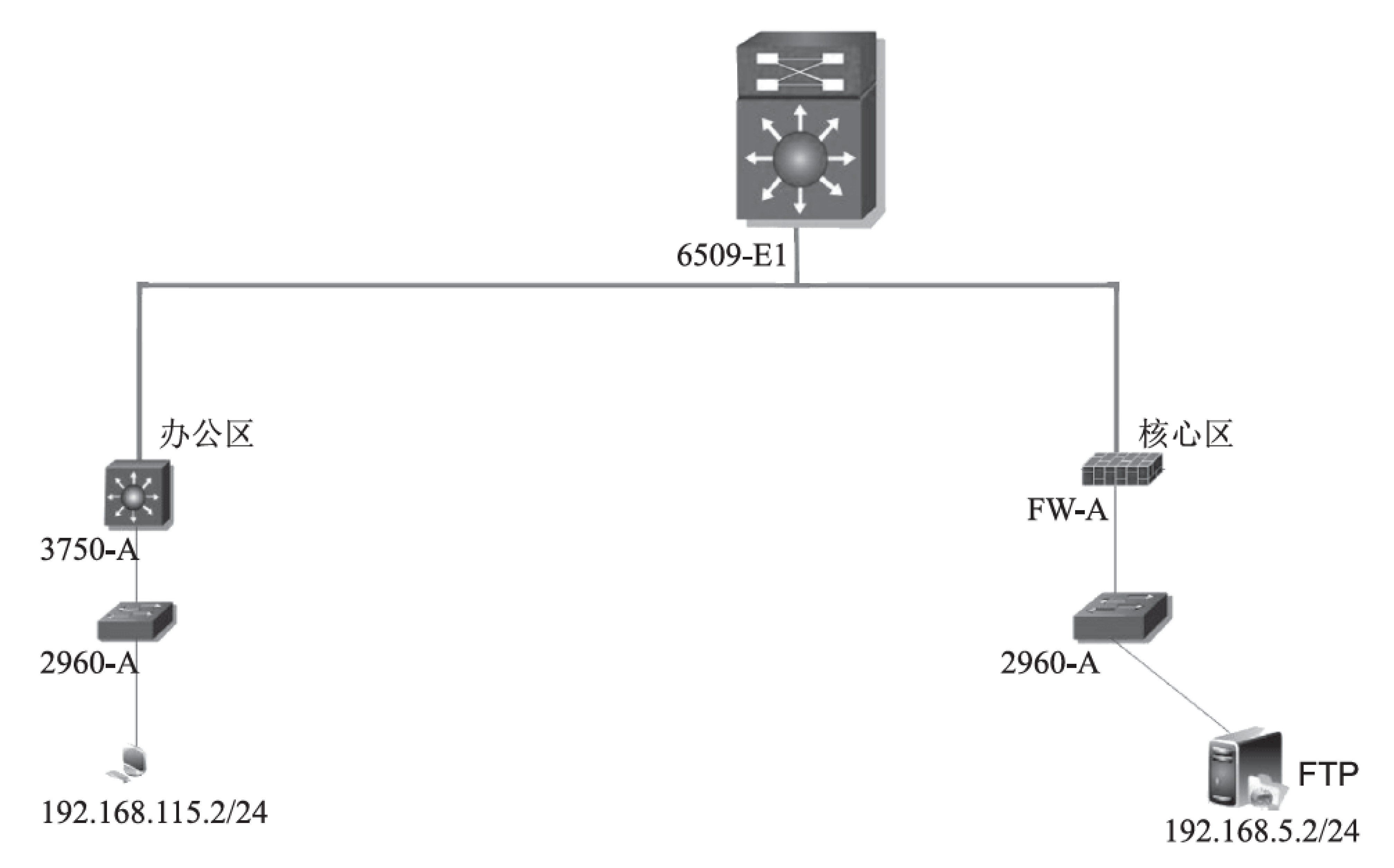


图4-8　可能发生故障的网络简洁拓扑图

第一步：在办公区用户的PC“命令行”CMD中执行命令“telnet 192.168.5.2 21”得到的输出结果为：

“正在连接192.168.5.2...无法打开到主机的连接。 在端口 21: 连接失败”。

这就说明在PC上不能登录到FTP服务器的21端口上。原因可能有很多种，可能是用户PC和FTP服务器之间的网络不通，也可能是FTP服务器上的21端口根本就没有打开。

第二步：确定是不是网络的故障。在办公区用户的PC“命令行”CMD中执行命令“ping 192.168.5.2”，得到如下的输出结果：

```
C:\Users\Administrator>ping 192.168.5.2
正在 Ping 192.168.5.2 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。
192.168.5.2 的 Ping 统计信息:
数据包: 已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)
```

从上面的输出结果可以看出PC和FTP服务器之间的网络是不通的。既然不通就要找出在图4-8中的“一条线”中到底是在哪个设备上出了问题。

第三步：在办公区用户PC的“命令行”CMD中执行命令“tracert 192.168.5.2”，它可以定位到数据包在传输过程中到底在哪个设备上出了问题。执行命令得到如下的输出结果：

```
C:\Users\Administrator>tracert 192.168.5.2
通过最多 30 个跃点跟踪到 192.168.5.2 的路由
```

```
  1     1 ms    <1 毫秒   <1 毫秒   192.168.115.254
  2      *        *          *       请求超时
  3      *        *          *       请求超时
```

上面的输出在第“3”行的下面本来还有很多，都省略了。因为数据包不能成功到达目的地192.168.5.2，所以它只能像第“3”行那样往下延续地输出。从输出的结果可以看出，PC上发出的数据包只能到达Cisco6509上，因为第“1”行输出中的192.168.115.254就是6509上VLAN 115的IP地址。也就是PC和6509之间的路由是通的，为了验证这个结果，我们在PC的命令行中执行了命令“ping 192.168.115.254”，结果能成功ping通。

其实，这也很好理解，PC发出的数据包，通过两个交换机Cisco2960和Cisco3750的二层广播功能，直接把数据包发送到了6509的三层端口VLAN 115上，VLAN 115收到数据包后发现是ping命令，就再把收到的数据包返回给PC。所以，在PC上能ping通6509。但是，从电脑PC上发出的ping数据包，在6509上就不能路由到FTP服务器，因为从执行命令“tracert 192.168.5.2”，输出的第“2”行一直往下，收不到返回的数据包。所以现在可以把故障定位在6509和FTP服务器之间。

第四步：这一步需要确定是不是因为FTP服务器引起的这种故障现象。所以就找了一台状态良好的笔记本电脑，把插在FTP服务器上的网线拔下来插到笔记本电脑的网口上，然后把笔记本电脑网口的IP地址、子网掩码和默认网关都配置成和FTP服务器完全一样的。然后，再次在办公区的电脑上执行和上面一样的ping命令、Telent命令和Tracert命令。结果与上面前三步的测试结果一样，还是不通。这就排除了FTP服务器引起的这种故障现象。其实，在这一步中所使用排除故障的方法，就是最简单，也是最常用的“替换法”。

第五步：因为在6509和FTP服务器之间，所经过的网络设备就只有6509、防火墙和2960，而2960上都是非常简单的二层配置，出现错误配置的可能性不大。6509在前三步的测试中，也没有发现有什么异常现象。所以问题最有可能出在防火墙上。

打开防火墙的WEB管理配置界面，查看其中的安全策略配置，发现其中并

没有配置允许192.168.115.2访问192.168.5.2的策略。因为所使用的防火墙策略，默认是全禁止的，也就是默认情况下防火墙不允许任何数据包通过，除非在它上面配置了允许某个数据包通过的策略。所以，只要在防火墙上添加了允许办公区用户访问FTP服务器的安全策略，就可以解决上面的问题。同时也要添加允许192.168.115.2的IP地址ping地址192.168.5.2的策略，这样在PC上也就能ping通FTP服务器了。

4. 防火墙上安全策略的配置。

在防火墙上总共需要配置添加两个策略，才能解决上面的故障，如下步骤所示。

(1)在防火墙上添加允许办公区用户访问FTP服务器的安全策略。如图4-9所示，是添加策略的Web界面。标红色星号的选项是必须填写的。“规则名”为VLAN115-to-VLAN5；“序号”是自动生成的；“源地址”和“目的地址”的IP地址和子网掩码就按如图4-9所示的填写即可，但注意子网掩码一定要写255.255.255.255，不能写成255.255.255.0。因为前者的子网掩码只对应一个IP地址，而后者则对应的是一个网段。如果把源地址和它的子网掩码写成192.168.115.2和255.255.255.255，意思就是只允许192.168.115.2这一个IP地址访问FTP服务器。但若是把子网掩码写成了255.255.255.0，那对应的安全策略就成了允许所有属于192.168.115.0/24这个网段的IP地址访问FTP服务器。



图4-9 在防火墙WEB管理界面中添加允许访问FTP服务

“动作”共有4个选项，但只能选择其中一项，“允许”就是允许与源地址和目的地址匹配的IP数据包通过，“禁止”就是不允许通过。还有两个选项是在防火墙上使用其他的安全功能时才选择的。最后一个选项是“服务”，这个是从服务的下拉菜单中选择的，选择的是ftp服务。一般在防火墙之类的安全设备上

都会默认定义一些常用的安全服务，如FTP、HTTP和ICMP等。另外，还有如下所示几个功能，虽然在本例中没有使用，但也非常重要。

“源端口”中端口号的填写，可以用英文逗号分割表示多个端口，或用英文冒号分割表示端口段。两种分割方式不能同时使用。“源MAC”是指数据包中二层的源MAC地址。

“流入网口”是限制网络数据包的流入网口，可以防止IP欺骗。可选内容包括：any和所有已激活的网口。默认值为any，表示不限制接收网口。如果防火墙工作在透明模式，必须选择相应的物理网口如Gi1。如果不能确定流入网口或工作在混合模式，就选择any。

“流出网口”流出网口检查，当选择源地址转换时才能选择。在透明模式下需要选择桥设备。如果不能确定流出网口或工作在混合模式，应当选择any。

“时间调度”是指在指定的时间段内，安全规则为生效状态，在指定的时间段外，安全规则就变为无效。

(2)在防火墙上添加允许所有的ping命令都能通过防火墙的策略。如图4-10所示，是在防火墙的WEB管理界面中添加此策略的示意图。“规则名”为ICMP；“序号”为18，也是系统自动生成的；注意“源地址”和“目的地址”中的IP地址、子网掩码任何内容都没有填写。其实这种情况下，不输入任何地址就代表所有的IP地址。也就是所有ping的数据包，无论它的源地址和目的地址是什么IP地址，都允许它通过防火墙；“动作”选择允许；“服务”选择的是icmp_any，它代表的就是ping命令所使用的服务。在图4-10中的还有以下的几个功能选项在本例中也是没有使用，但也非常重要。

“长连接”设定该条规则可以支持的长连接时间。0为不限时。若限时，则有效的时间范围是30～288000分钟。如果希望在指定的时间之后断开连接，就可以设定该功能。

“深度过滤”在生效的安全规则中执行深度过滤。不过，对数据包进行应用层的过滤会影响系统的处理性能，所以一般情况下不要启用深度过滤。可以在下拉框的选项中选择“无”，从而不启用深度过滤功能。

“P2P过滤”对满足条件的数据包进行BT过滤。Emule和Edonkey过滤，只在包过滤“允许”的情况下可用，至少选择“BT过滤”、“Emule和Edonkey过

滤”的其中一个时，才可以选择“P2P日志纪录”。

图4-10　在WEB管理界面中添加允许Ping包通过防火墙

这里BT过滤就是对于满足该规则的连接，禁止其BT下载，支持的BT客户端包括BitComet 0.60以下版本、BitTorrent和比特精灵。Emule和Edonkey过滤就是对于满足该规则的连接，禁止其Emule和Edonkey下载。不过，对于已经建立连接的BT/ed2K的下载，不能禁止，必须重启BT/ed2K客户端后才能生效。

“抗攻击”共包括4种抗攻击。TCP服务可以选择抗SYN Flood攻击；UDP服务可以选择抗UDP Flood攻击；ICMP服务可以选择抗ICMP Flood攻击和抗Ping of Death攻击。也可以在一条规则中，选择多个抗攻击选项。4种抗攻击的详细说明如下：

当允许TCP规则时，选择了抗SYN Flood攻击，防火墙会对流经的带有Syn标记的数据进行单独的处理。抗Syn Flood攻击之后的输入框填写数值的具体含义：个位数为保留数字，0～9分别代表抗攻击强度，从弱到强。设置数字的位数如果超过两位，则该数字减去个位的数字表示限制每秒通过的能够真正建立TCP连接的带有Syn标志数据包的个数。如果设置为0，表示每秒通过的带有Syn标志的数据包大于90，才进行能否真正建立TCP连接；如果设置为1，表示每秒通过的带有Syn标志的数据包大于80，才进行能否真正建立TCP连接；如果设置为9，表示

通过的带有Syn标志的数据包都经过了防火墙的判断，确认是可以建立真正TCP连接的数据包。

当允许UDP规则时，选择了抗UDP Flood攻击，防火墙会对流经的UDP数据进行单独的处理。抗UDP Flood攻击之后的输入框填写的数值的具体含义是限制每秒通过的UDP数据包的个数。

当允许ICMP规则时，选择了抗ICMP Flood攻击，防火墙会对流经的ICMP数据包进行单独的处理。抗ICMP Flood攻击之后的输入框填写的数值的具体含义是限制每秒通过的ICMP数据包的个数。

当允许ICMP规则时，选择了抗ping of Death攻击，防火墙会对流经的ICMP数据包进行单独的处理。含有ping of Death 攻击特征类型的数据包将被过滤掉。

“包过滤日志”强制要求匹配该条规则的数据包是否需要记录包过滤日志。

(3)在防火墙的WEB管理界面中，配置添加完以上两条安全策略后，也就解决了在办公区用户的电脑上不能ping通和不能访问FTP服务器上资源的故障。

5. 总结

(1)随着互联网的飞速发展，网络安全问题越来越突出，人们的安全意识也不断地提高，但现在还没有一项技术和工具比防火墙解决网络的安全问题更有效。利用它强大的隔离和预防作用，通过在网络边界进行隔离，是改善网路安全状况最有效的方式。防火墙通常是圈定一个保护的范围，并假定防火墙是唯一的出口，然后防火墙来决定是放行还是封锁进出的数据包。

防火墙不是万能的，但没有防火墙是万万不能的。防火墙不能解决所有的安全问题， 但防火墙解决了绝大部分的安全问题。再配合其他的安全技术和工具，它能够提供完整的安全解决方案。随着互联网应用的增加，标准软件的漏洞也越来越多，这种隐患不但没有很好地解决，而且情况越来越严重，通过部署防火墙来屏蔽这种问题，目前还是最有效的手段。

(2)以上所述，都是目前广泛使用的传统型防火墙在网络中所发挥的巨大作用及其优势，但是这些传统防火墙都是基于一种重要的理论假设来进行安全防护的。这种理论认为如果防火墙拒绝某类数据包的通过，则认为它一定是安全的，因为该类包已经被丢弃。但防火墙并不保证准许通过的数据包是安全的，它无法判断一个正常的服务的数据包和一个恶意的数据包有什么不同。传统防火墙也无

法提供基于应用和用户的，从第三层到第七层的一体化访问策略控制，黑客常常通过穿透合法的80端口，就可以轻松地让防火墙的安全控制策略变成“聋子和瞎子”。此外，它也无法提供基于应用的流量分析和报表展示，无法帮助用户了解当前网络边界的现状。而且，当前的安全威胁已不再是单一的类型。通常一个完整的入侵行为包含了多种技术手段，如漏洞利用、WEB入侵、木马后门、恶意网站等，如果将这些安全威胁割裂地进行处理和分析，系统的防范短板依然存在。

新一代的防火墙应该加强，允许通过防火墙的数据包的安全性，因为网络安全的真实需求是，既要保证网络安全，也必须保证应用的正常运行。所以，目前企业使用越来越多的七层防火墙受到了更多人的关注，它是一种基于应用层开发的新一代应用防火墙，与传统安全设备相比它可以针对丰富的应用提供完整的、可视化的内容安全保护方案。它解决了传统安全设备在应用可视化、应用管控、应用防护、未知威胁处理方面的巨大不足，并且满足了同时开启所有功能后性能不会大幅下降的要求。七层防火墙既满足了普遍互联网边界行为管控的要求，同时还满足了在内网数据中心和广域网边界的部署要求，可以识别和控制丰富的内网应用。

相信，随着人们对网安全意识的不断增强和各种功能强大、性能先进安全设备的广泛应用，一个安全、绿色的互联网会越来越深入到人们的工作和生活当中。

4.3 运维实例：UTM双机热备和虚拟域功能

目前，人们在享受网络带给人们工作、生活种种便利的同时，也饱受着各种各样网络安全问题的威胁，例如病毒、蠕虫、垃圾邮件、网站钓鱼和间谍软件等。针对这些不安全的因素，我们需要在网络中部署不同的设备去对付它，例如防火墙、IPS、VPN、IDS和漏洞扫描等。但同时部署这些不能相互通信的多种网络安全产品，不仅提高了网络的复杂性，而且还增加了管理操作成本。这其实不是最佳的部署模式。

UTM(Unified Threat Management，统一威胁管理)就很好地解决了上面的问题。它在一个硬件装置中集成了多种安全特性，带有防病毒、网络入侵监测、防

垃圾邮件、VPN和Web过滤等功能。所有这些功能不需要一定被启用，但这些功能都集成在了UTM硬件上，一旦需要使用的话，只需开启即可。UTM在网络中的部署，增强了全面保护网络服务的灵活性，同时也降低了部署的复杂度。下面就以两则实例介绍UTM在实际中的应用。

1. UTM双机热备部署模式的应用

(1)UTM双机热备的总体部署情况。如图4-11所示，网络的核心层和接入层分别使用了两台Cisco4506和两台Cisco3560交换机，在Cisco3560上接入有多个用户组，根据用户组所属部门的不同把他们划入到不同的VLAN中。在Cisco4506和Cisco3750之间接入了两台联想Power V UTM。两台Cisco4506之间和两台Cisco3560之间都是Trunk连接。设备间的连接情况如下所示：

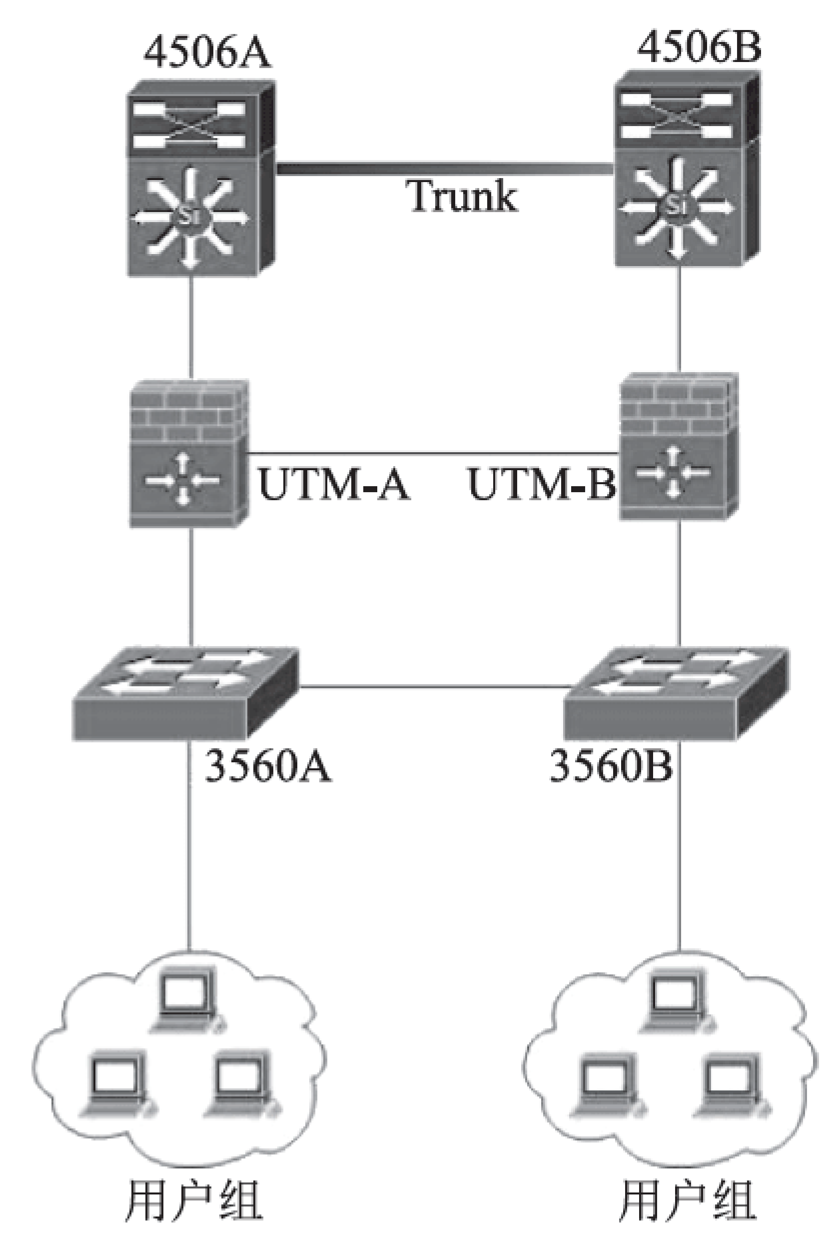


图4-11　UTM双机热备模式部署图

```
Cisco4506A GigabitEthernet6/1 <----> UTM-A  Port 1
Cisco4506B GigabitEthernet6/1 <----> UTM-B  Port 1
Cisco3560A GigabitEthernet1/0/1 <----> UTM-A  Port 2
Cisco3560B GigabitEthernet1/0/1 <----> UTM-B  Port 2
UTM-A  Port 10 <----> UTM-B  Port 10
```

联想UTM设备支持在路由和透明模式下的主备和主主模式的高可用性配置，但它不支持全冗余的连接模式。在图4-11中，UTM工作于路由模式，HA监控Port 1和Port 2两个接口。两个UTM使用Port 10接口作为HA的心跳线接口。

两台Cisco4506之间使用了思科专有协议HSRP，这样当任意一台4506故障，并不会影响网络中每个用户组对网络的正常访问。例如现在图4-11中，两台Cisco4506因为使用HSRP协议，4506B处于备用状态，而4506A处于活动状态，也就是说Cisco4506A具有三层路由功能，而4506B只有二层交换功能，不具备路由功能。

如果Cisco4506A因为某种原因发生故障，整个交换机宕掉，因为HSRP协议的作用，Cisco4506B马上会启用它自身的三层路由功能，从而接管4506A上的各种功能。若这时处于活动状态的UTM是UTM-A，因为4506A已经宕机，UTM-A就能监控到它上面的Port 1端口上已经没有数据，又因为HA一直监控Port 1和Port 2，所以这时HA就会启用UTM-B，让它由备用状态变为活动状态，而UTM-A由活动状态变为备用状态。这时连接到3560交换机上的用户组，原来访问核心交换机的数据都是通过UTM-A传输的，现在都改成通过UTM-B再传输到核心交换机。所以说图4-11中的配置模式，无论是核心交换机，或是UTM中的任意一台发生故障都不会影响到全网用户对网络的正常访问。Cisco3560因为是接入层交换机，所以对它的可靠性要求不是很高，若其中的一台故障的话只会影响到很少一部分用户，所以Cisco3560没有配置成负载均衡，或者是双机热备的模式。

在部署UTM双机热备模式时需要注意：双机热备中的UTM，必须是相同型号和相同软件版本的UTM才可以作双机热备；主主模式(Active—Active)的双机热备，支持对TCP会话的负载均衡；在双机热备的具体配置中，不要使用主设备的抢占模式。因为主UTM往往能抢占成功，但主UTM中的防火墙却不抢占，所以应用主设备抢占模式往往会导致UTM在功能应用上的混乱。

(2)UTM双机热备的配置步骤。

①网络接口配置。因为在图4-11的部署模式中，两台UTM就相当于一台路由器，所以可以在UTM的WEB管理界面中的“系统管理”→“网络”→“接口”中，把Port 1和Port 2两个端口配置到不同的网段中，Port 1的IP地址为172.16.2.1，子网掩码为255.255.255.0，Port 2的IP地址为172.16.3.1，子网掩码为255.255.255.0。这时Port 1就位于网络172.16.2.0/24中，而Port 2就位于网络

172.16.3.0/24中。

同时，接入到Cisco3560上的用户组IP地址也都可以划入到网络172.16.3.0/24中。这样只需要在UTM上配置172.16.2.0/24和172.16.3.0/24两个网络可以互相访问的路由，就可以实现3560上的用户组对核心交换机的正常访问。Port 10接口作为UTM设备的心跳线接口，可以不配置IP地址。

②HA参数的具体配置。可以在UTM的WEB管理界面的“系统管理”→“配置”→“高可靠性”中对HA参数进行具体的配置。如图4-12所示，“高可靠性”的模式可以有三种选择，“单独”“主动—被动”和“主动—主动”。在本例中选择“主动—被动”的模式，也就是双机热备的工作模式。其他参数的配置如图4-13所示。

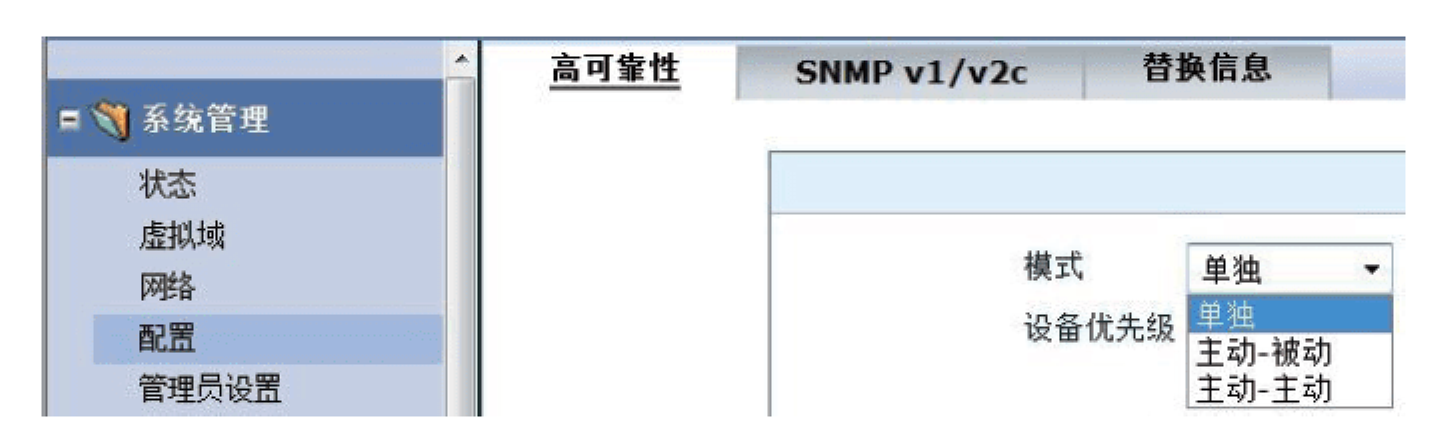


图4-12　部署UTM的三种模式



图4-13　UTM双机热备HA参数的配置

设备优先级：缺省为128，优先级的值越高设备被选择为主设备的机会越大，可以根据实际的网络环境确定是否需要确定首选主设备。图中还有“虚拟集群”的选项，这也是联想Power V UTM上的一种功能，可以把一台物理UTM设备虚拟成两台独立的逻辑UTM设备来使用，这将在第“2”点中进行详细介绍。

密码：为HA同步的通信密码，两台UTM设备必须设置相同的密码。

端口监控：为UTM设备检测端口，当该端口down时，设备切换。注意在没有完成双机协商前，不要配置“端口监控”。待设备完成双机同步后再配置“端口监控”。

心跳线接口：为HA设备的双机热备接口，填写数值的接口表示该接口支持双机热备，数值大的为主心跳接口。

③互连两台UTM设备。用一根直通网线，也就是一根两端线序一样的双绞线，连接两个UTM设备的Port 10端口，并要保证双机线的畅通。UTM设备在进行双机热备工作时，只有主设备可以被管理，而且所有的配置均在主设备上完成，它会把配置自动同步到备用设备上。

④创建安全访问策略。也就是在UTM的WEB管理界面中的“防火墙”中配置将要在网络中应用的安全策略。例如，可以在“防火墙”中配置禁止连接在Cisco3560上的某个VLAN中的用户访问核心交换机上的数据。同时，所有在主UTM上配置的策略会自动在两台设备上同步。

⑤双机热备的切换测试。若拔出接在UTM-A设备Port 1或Port 2上的网线，正常情况下活动的UTM设备就会切换到UTM-B上。然后重新访问UTM设备的管理IP地址，就可以观察到主、从UTM设备的切换情况。如果想要管理双机热备中的从UTM设备，就只能通过CLI命令行的方式进行管理。先要登录到主设备上，然后再在主设备的CLI下对从设备的UTM进行管理。

(3)小结。

①UTM HA集群。集群是由两台或更多的UTM设备组成一个HA集群。对于网络而言，HA集群可以对外界表现为单个UTM处理网络数据传输并提供常规的安全服务，如防火墙功能、VPN、IPS、病毒检测、Web过滤和垃圾邮件过滤服务。

在HA集群中，单个的UTM设备称作为一个群集UTM。这些UTM共享安全

策略与配置信息。如果一个群集UTM发生故障，集群中的其他UTM自动替换故障的UTM，承担该UTM所做的工作。群集将继续处理网络数据传输，并不间断提供网络安全服务。HA集群包括一台主要的群集UTM，也称为主UTM，与一台或更多的从属群集UTM，也称从属UTM。主UTM控制着整个群集的操作，根据群集的操作模式，主UTM发挥着不同的作用。

HA集群在发生故障后仍能够继续提供UTM功能的特性称作故障转移。UTM HA故障转移意味着你的网络不需要依赖一台UTM提供服务，可以安装额外的UTM组成一个HA集群。HA集群的另一个功能是负载均衡，该功能可以提高网络的使用效率。UTM群集通过分担处理网络流量并提供安全服务增强整个网络的性能。在网络中，群集可以作为单一UTM，不需要更改网络配置便可以增强网络的使用效率。

②UTM HA模式。联想POWER V UTM防火墙能够配置运行于“主动—被动(A-P)”，或“主动—主动(A-A)”模式。“主—主”和“主—被”模式群集都能够运行于UTM的NAT/路由或是透明工作模式。“主动—被动(A—P)”模式集群，是由一台处理网络流量的主UTM以及一台或多台从属UTM组成。从属UTM和主UTM连接，但并不处理数据传输。“主动—主动(A—A)”模式负载平衡所有群集UTM的网络流量。一个主动—主动HA群集由一台处理数据传输的主UTM以及一台或多台也同样进行数据传输处理的从属UTM组成。主UTM使用负载平衡策略分布并平衡HA群集中所有UTM的流量处理。

2. UTM虚拟域功能的应用

(1)使用UTM虚拟域前的网络部署情况。单位在部署使用UTM虚拟域功能之前，有两个相互独立的网络，外网和专用网，网络部署图如图4-14和图4-15所示。两个网络共使用了三台联想Power V UTM，外网中两台，专用网中一台。

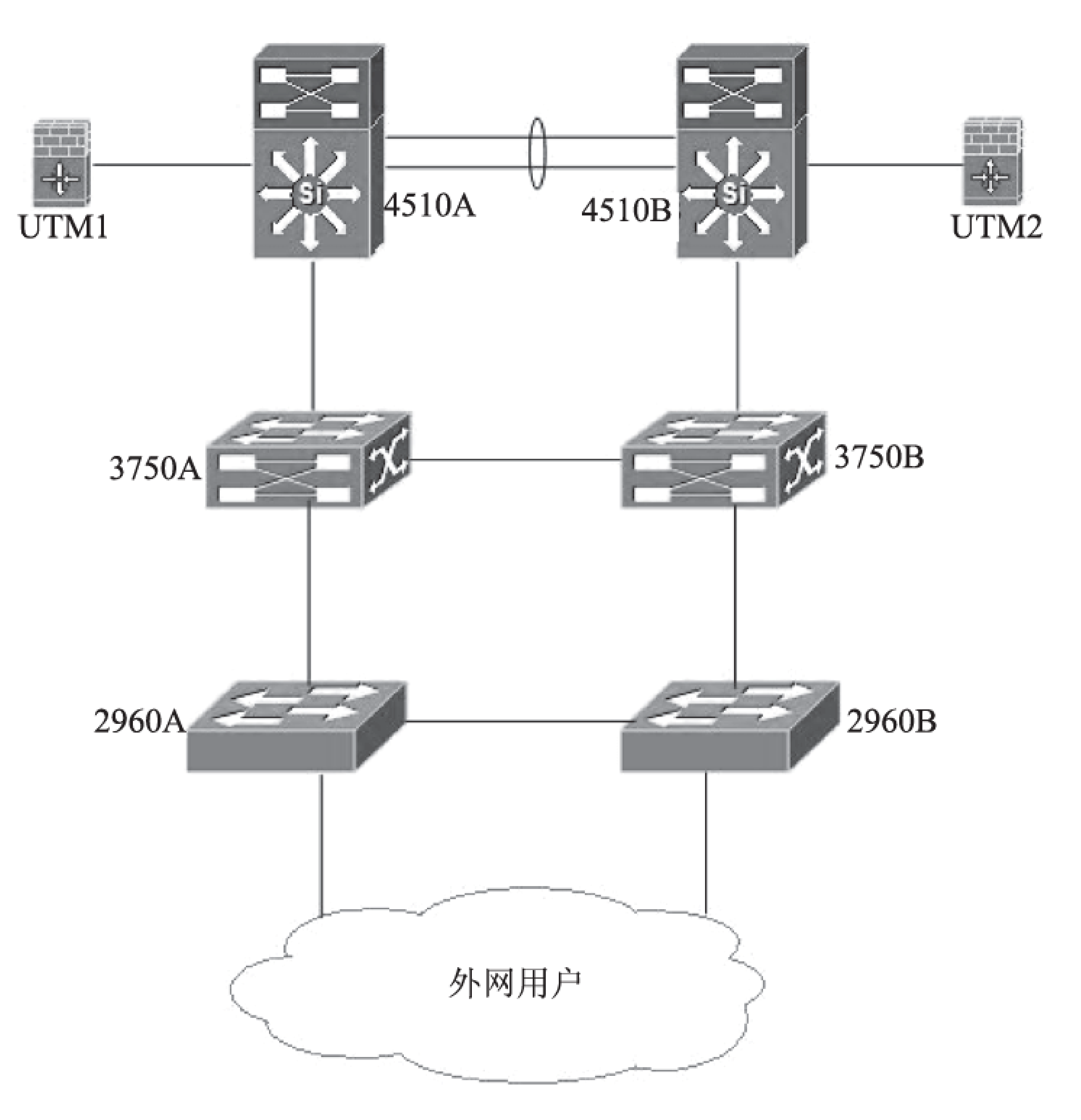


图4-14　使用UTM虚拟域功能前外网图示

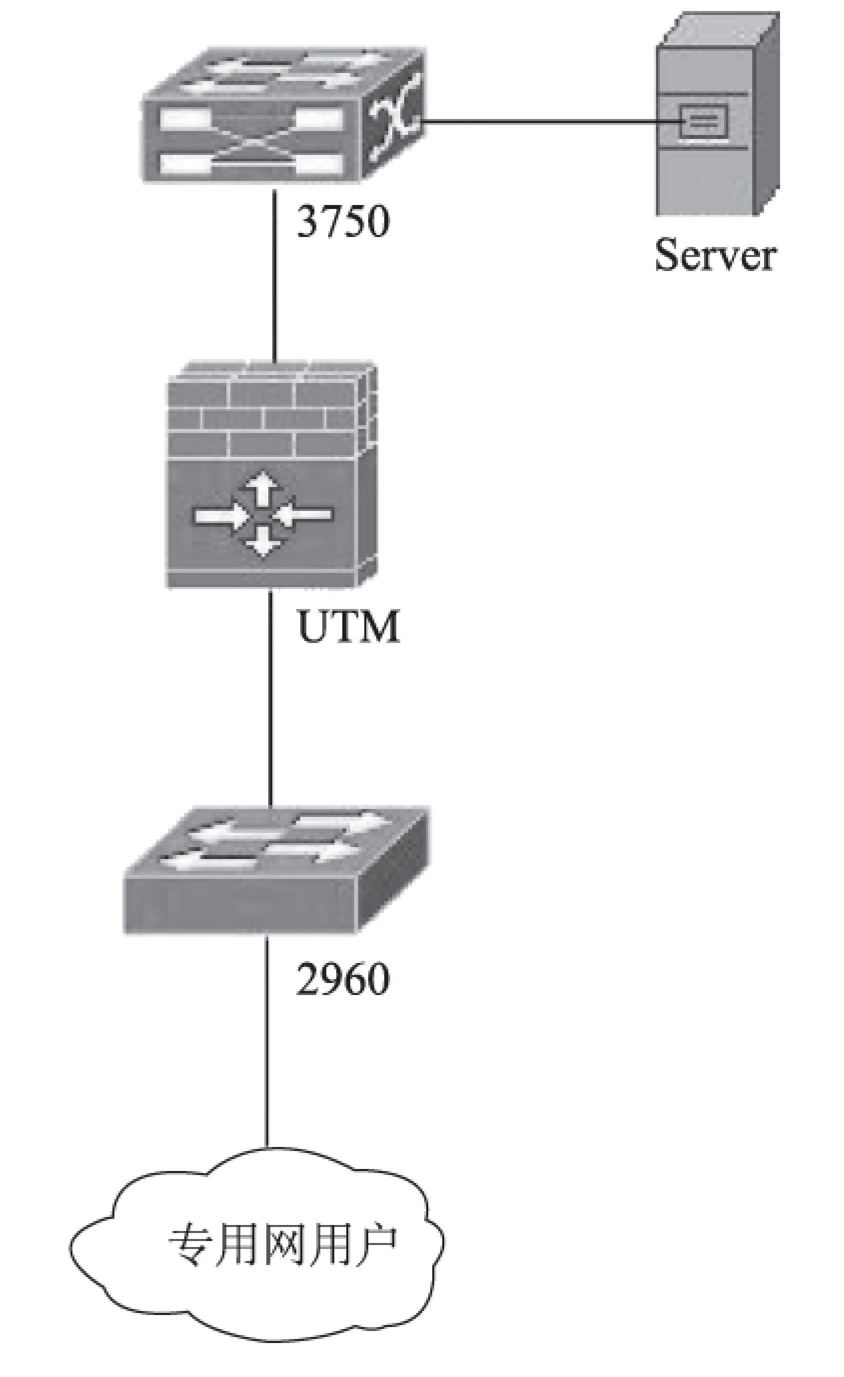


图4-15　使用UTM虚拟域功能前专用网图示

Power V UTM工作模式共有两种，NAT/路由模式和透明模式，如图4-16所示。外网两台UTM部署的是双机热备，工作模式是NAT/路由模式，具有路由功能，也就是UTM同时也相当于一台路由器，能学习路由，转发数据包，本身作为三层设备参与到用户环境中，可以控制多个VLAN之间的数据包流，对收到的数据包，能根据其目的IP地址进行转发。NAT/路由模式还支持UTM设备与802.1Q交换机、路由器之间创建VLAN Trunk，提高了用户对设备配置的灵活性。在图4-14中的UTM1和UTM2之间还有直接相连的心跳线，图示为了简洁没有画出。心跳线的作用是为了实现两台UTM设备的双机热备功能。在运行中主UTM会将状态信息、NAT信息备份到备用UTM中，若发生切换，备用UTM会保存完整的NAT转换信息，从而不会导致用户访问网络数据的中断。



图4-16　UTM的两种工作模式

在图4-14的逻辑拓扑图中，UTM1和UTM2分别与两台Cisco4510的连接，图中只画出了一条连接线。在实际的部署中，每一台UTM和Cisco4510的连接都有两根连接线。例如UTM1的Port 1、Port 2分别和Cisco4510A的Gi6/1、Gi6/2相连，其中Port 1和Gi6/1都是Trunk口，也就是二层端口，端口上都没有配置IP地址，它们之间属于Trunk连接。但在Port 1下可以配置多个三层的VLAN子接口，同时在这些子接口上也可以配置相应的IP地址。而Port 2是属于三层端口，它上面也配置了IP地址，Cisco4510的Gi6/2端口，可以划入到4510A上的某个VLAN中。这样配置后，Port 1下面的多个三层VLAN子接口，就可以和Port 2的三层端口之间相互通信，因为它们都有IP地址，都属于某个子网，只有它们之间有可达路由，就可以相互访问。若不想让Port 1下面的某个三层VLAN子接口和Port 2之间进行通信，就可以在UTM上配置相应的安全策略，从而阻止它们之间的相互访问。这也就是UTM设备，以旁路的方式接入到核心路由或交换设备上，并能实现UTM设备的三层路由功能的部署模式。最终通过在UTM设备的防火墙中配置安全策略，实现允许/禁止某类用户对特定数据的访问。

而图4-15专用网中UTM的工作模式是透明模式，它是以“桥”模式运行的，

本身只需要配置一个管理IP地址，不必占用任何其他的IP资源，也不需要改变用户的拓扑环境，设备的运行对用户来说是“透明”的，在网络设备上进行各种命令的配置时，就当不存在这个UTM一样，因为它是透明模式。它只对线路上的数据作安全检查和安全策略上的限制，本身不会影响网络的整体架构和配置。这种模式在安装和维护UTM时，相对路由模式来说要简单很多。

因为单位在安全方面的严格要求，专用网中必须使用UTM设备。但是目前专用网中只有一台UTM，一旦UTM发生故障后，专用网将面临无安全防护的隐患。这种情况下，也可以考虑再购买一台和专用网中一模一样的UTM设备，这样把两台设备配置为双机热备或负载均衡的模式，就是把买来的UTM作为冷备也可以。这样当其中的一台故障后，另外一台就可以马上替换掉有故障的一台。但一台UTM设备，因为它上面集成了多种安全功能，所以在价格方面也非常昂贵，一台至少也要十多万人民币，而单位经费紧张，所以考虑买UTM设备的办法行不通。我们经过查阅联想UTM的各种随机文档，发现它具有“UTM虚拟域”的功能。

其实，UTM虚拟域功能就是可以把一台UTM物理设备划分为多个虚拟域，每个虚拟域在逻辑上就相当于一台单独UTM物理设备，每个虚拟域也可以单独设置路由、防火墙策略、防病毒策略、IPS策略等。这样就可以为多个企业组织部署一个UTM，将其划分成若干个逻辑设备分配给不同的企业组织，并且为其设置相应的逻辑设备管理权限，这样每个被服务的企业组织可以单独管理安全设置，并查看相应的日志信息。

(2)配置UTM虚拟域的具体步骤。

①在UTM WEB管理界面中的“系统管理”→“状态”界面中，首先要启用虚拟域功能，当然要是不想使用虚拟域的功能，也可在此选择停用其功能。图示中的“虚拟域”功能已经启用，单击“停用”就中止了UTM的虚拟域功能。

②在“系统管理”→“虚拟域”的管理界面中，单击“新建”的功能按钮，就能新建一个UTM虚拟域，并填写虚拟域的名称为ca，并配置虚拟域ca的“工作模式”为透明模式，如图4-17所示。

③在“系统管理”→“网络”→“接口”的管理界面中，单击将要放入虚拟域ca的某接口的“编辑”功能按钮，在“虚拟域”的下拉菜单中选择虚拟域ca，如图4-18所示。



图4-17　新建虚拟域图示



图4-18　把端口划入到相应的虚拟域中

④在新建的虚拟域中，配置防火墙的安全策略、防病毒功能和入侵检测功能。

⑤把专用网中，原来连接在专用网中的Cisco3750和Cisco2960上的两根接入到UTM上的网线，连接到UTM2上新建虚拟域中的相应端口上。

(3)使用UTM虚拟域后的网络部署情况。改造后的网络结构图如图4-19所示。从图中可以看出，UTM2处于活动状态，也就是主UTM，而UTM1处于备用状态。因为在主UTM上所做的任何配置，都会同步到备用的UTM上，也就是在UTM1上也有一个和在UTM2上一模一样的虚拟域，此虚拟域也和原来专用网中的UTM功能是一样的。这样如果图4-19中的UTM2故障的话，因为双机热备模式的缘故，UTM1马上就从备用状态转变为活动状态，接管UTM2的各种业务，UTM2的状态也就从主UTM变成了备用状态。一旦UTM2变成了备用状态，在它上面的替代原来专用网中的UTM的虚拟域也就从活动状态变成了备用状态，因为整个UTM2设备的状态都成为备用的了。

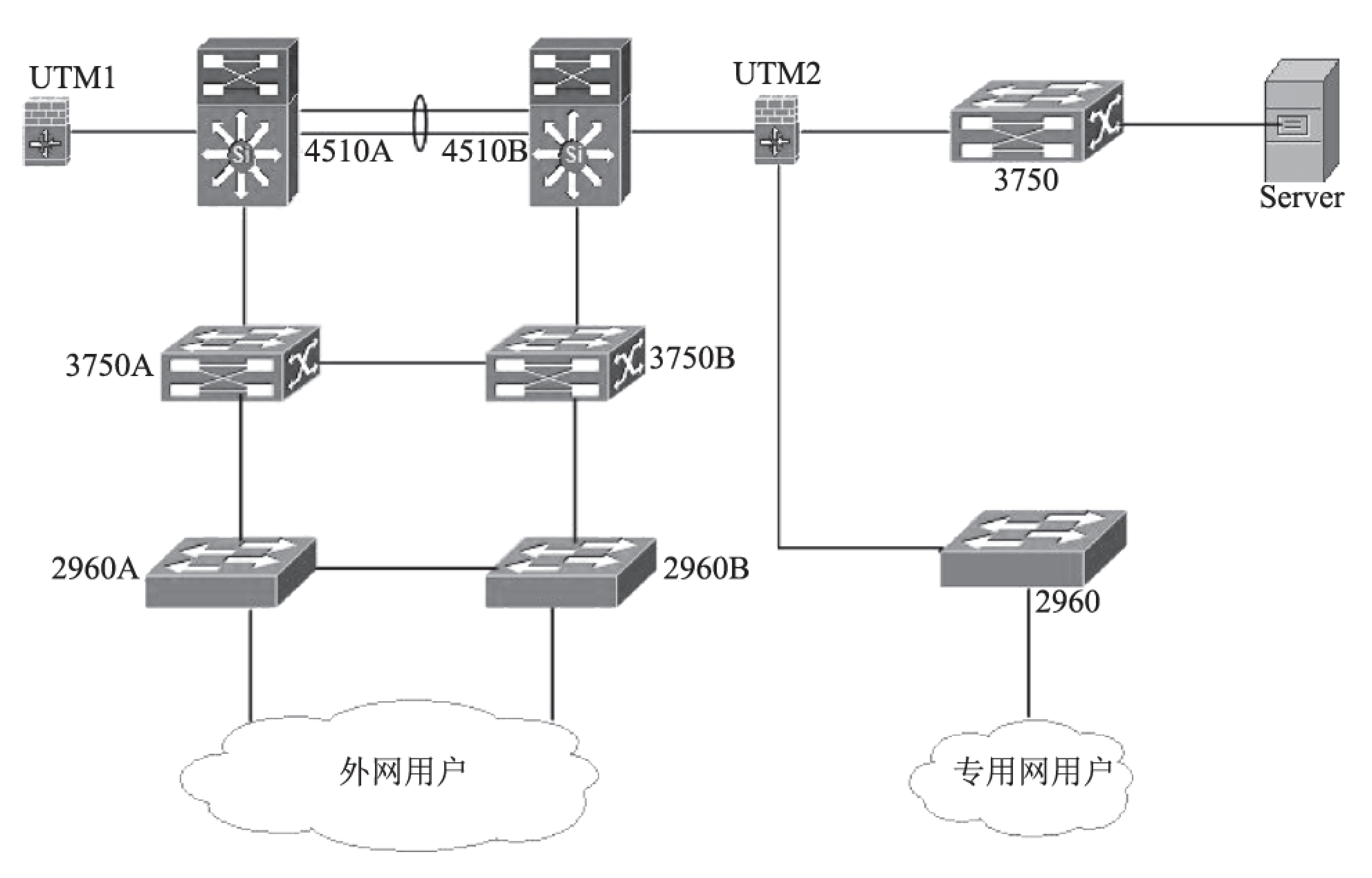


图4-19　使用UTM虚拟域后网络结构图

所以图4-19中，一旦UTM1和UTM2的运行状态发生变化后，网络工程师一定要尽快把接在专用网中两个交换机上的连接UTM2的两根网线，接入到UTM1上对应的虚拟域的端口上。这样才能保证专用网再次安全稳定地运行。启用UTM虚拟域功能前的原来专用网中使用的UTM已经断电不再使用。但它可以作为图4-19中UTM1和UTM2的冷备。即使UTM1和UTM2两个设备都故障了，可以再把原来专用网中的UTM上电，同样可以保证专用网的安全正常访问。

UTM虚拟域功能的使用，在为单位节省一大笔经费的同时，也提高了专用网的安全性和可靠性。

(4)小结。

UTM设备功能很强大，几乎现在所有安全产品的功能在UTM中都能找到。它增强了网络的安全性，避免了网络资源的误用和滥用，在更有效地使用通信资源的同时，它也不会降低网络的性能。UTM也是易于管理的设备，它的功能包括：应用层服务，例如病毒防护、入侵检测、垃圾邮件过滤、网页内容过滤以及IM/P2P过滤服务；网络层服务，例如防火墙、入侵检测、IPSec与SSL VPN及流量控制；管理服务，例如用户认证、设备管理设置、安全的WEB与CLI管理访问以及SNMP功能。

但是建议在开启UTM虚拟域功能的同时，不要再使用UTM上的其他功能。因为虚拟域功能在逻辑上就相当于在不增加任何UTM硬件资源的情况下，又虚构出一个UTM设备，所以虚拟域功能会占用大量UTM设备上的CPU、内存等资源，这时若再启用UTM上的其他功能，必定会大大增加UTM的负荷，这其实也就给它的使用带来了不稳定因素。因为所有设备在超负荷的运行下，故障率都会大大增加。所以建议在没有特殊需求的情况下，使用UTM虚拟域功能时不要过多开启UTM上的其他功能。

4.4　运维实例：SSL VPN部署与排障

目前，越来越多的用户可以在远程通过互联网访问企业内部的资源。但单位内部的资源，常常因为安全性的要求，不能直接放置在Internet上。为了满足这种远程访问企业内部资源的需求，SSL VPN(Security Socket Layer Virtual Private Network，安全套接层虚拟专用网络)应运而生，它完全可以满足用户在这方面的需求。下面就以一家报社的分社，访问总社内网中FTP服务器资源为例，介绍SSL VPN的部署搭建、客户端的安装及其故障排除。

1. SSL VPN的部署情况

图4-20所示，是总社SSL VPN部署的基本架构拓扑图。SSL VPN设备放置在DMZ区，和DMZ区的交换机3750相连。FW-A和FW-B是DMZ区的两台防火墙，在网络的内部还部署有两台服务器的防火墙FW1和FW2。分社的用户位于全国的各个省份，他们通过Internet访问总社网络服务器的资源总共要经过以下四个阶段：

第一阶段：如图4-20所示，分社的用户PC通过Internet，把数据发送到Cisco 6503，6503再把数据包路由到防火墙FW-A或FW-B，然后经过Cisco3750，最后到达SSL VPN设备上。

第二阶段：SSL VPN设备收到分社用户PC访问的数据包，对数据包进行解封装后，知道它是要访问总社网络中的FTP服务器。然后SSL VPN设备就会发起一

个代理分社用户PC对FTP服务器的访问。通过3750、FW-A或FW-B、4506、FW1或FW2和2960，最终到达FTP服务器。

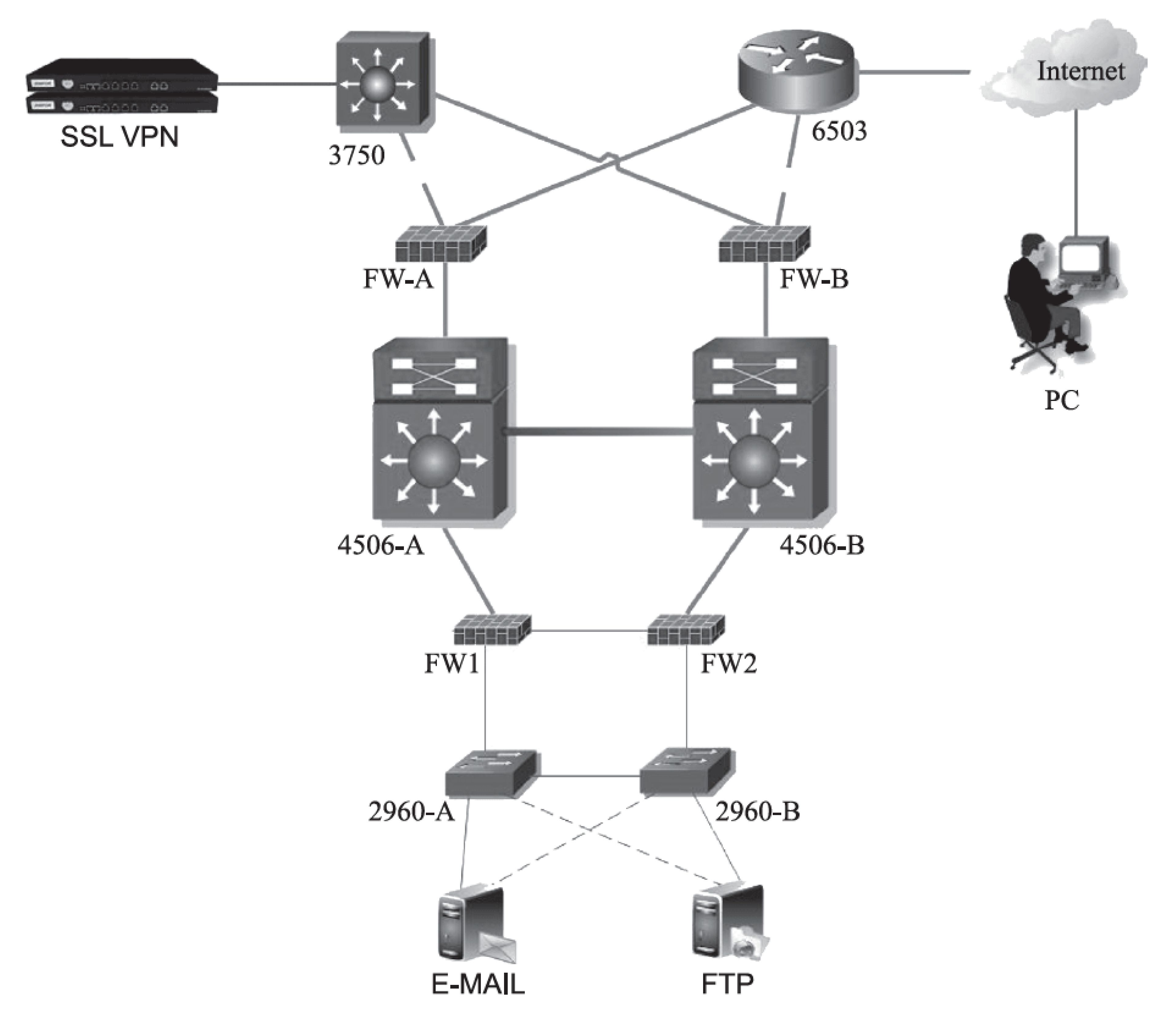


图4-20　SSL VPN网络部署拓扑图

第三阶段：这个阶段数据包的传输过程，其实和第二阶段数据包的传输方向正好相反。当SSL VPN访问的数据包到达FTP服务器后。FTP服务器需要对接收到的数据包进行处理，然后再把数据包重新封装返回给SSL VPN。数据传输的路径是通过2960交换机、FW1或FW2防火墙、4506交换机、FW-A或FW-B防火墙，然后再经过3750，最后到达SSL VPN。

第四阶段：当SSL VPN设备收到FTP服务器处理完的数据包后，就会把数据包返回给位于分社的用户PC。数据的流向是先经过3750、FW-A或FW-B防火墙、6503，然后通过互联网的传输，最终到达用户PC。

以上四个阶段就是分社用户通过Internet采用SSL VPN的方式访问单位内部服务器资源的一个完整过程。

2. SSL VPN客户端的部署与安装

部署SSL VPN网络，最复杂的是在SSL VPN设备上的配置，因为要在设备上面设置访问内网中各个服务器的IP地址和各种应用程序的端口号。但是随着SSL VPN功能的不断强大，通常在客户端也要进行以下两方面的配置。

(1)安装SSL VPN的客户端插件。如本例中使用的是深信服SSL VPN，当用户PC第一次用浏览器以https的方式访问总社内网资源时，会提示安装如图4-21所示的插件。如果不安装此插件的话，用户就不能在远程PC上使用SSL VPN的功能。而且，不同品牌的SSL VPN客户端插件，所实现的功能是不一样的，有的是在用户的PC上形成虚拟网卡，有的插件安装后会更改浏览器上的一些默认设置。



图4-21　SSL VPN客户端安装程序示意图

(2)在分社用户PC的桌面上，建立连接SSL VPN的快捷方式。在用户PC的浏览器地址栏中输入以https方式访问总社SSL VPN的地址后回车，进入到访问总社内网资源的首页面。然后在浏览器中依次单击“文件”→“发送”→“桌面快捷方式”后就可以在电脑的桌面上建立访问SSL VPN的快捷方式。这样下次再想使用SSL VPN时，只需直接打开桌面的SSL VPN快捷方式即可，不用再在浏览器的地址栏中输入访问总社网络资源的网址，方便快捷。

3. 排除分社使用SSL VPN访问总社内网资源速度慢的故障

因为把SSL VPN快捷方式和客户端驱动建立安装完成后，发现使用SSL VPN访问总社内网的资源速度非常慢，严重影响了分社用户的正常工作，很长时间都打不开网页页面。后来，经过多次的测试发现，分社用户在每天的下午访问互联网，包括使用SSL VPN访问总社内网的资源速度非常慢。但在每天的上午时间，

网络的速度比下午要好很多。而且这种现象是分社所有用户都是这种情况，并不是一部分用户或是个别用户访问速度慢。这就排除了网速慢的故障和用户的电脑没有关系，很可能是分社网络的问题。

后来经过查看分社的网络架构，发现分社是和另外的其他用户共用一互联网出口带宽。如图4-22所示，而且共用带宽的“其他用户”，因为工作原因，下午的时间是他们上网的高峰时段。所以当“其他用户”在高峰时段上网占用出口更多的带宽后，就会严重影响到分社用户访问互联网的速度，从而影响使用SSL VPN访问总社内网资源的速率。因为SSL VPN也是通过Internet传输数据的。

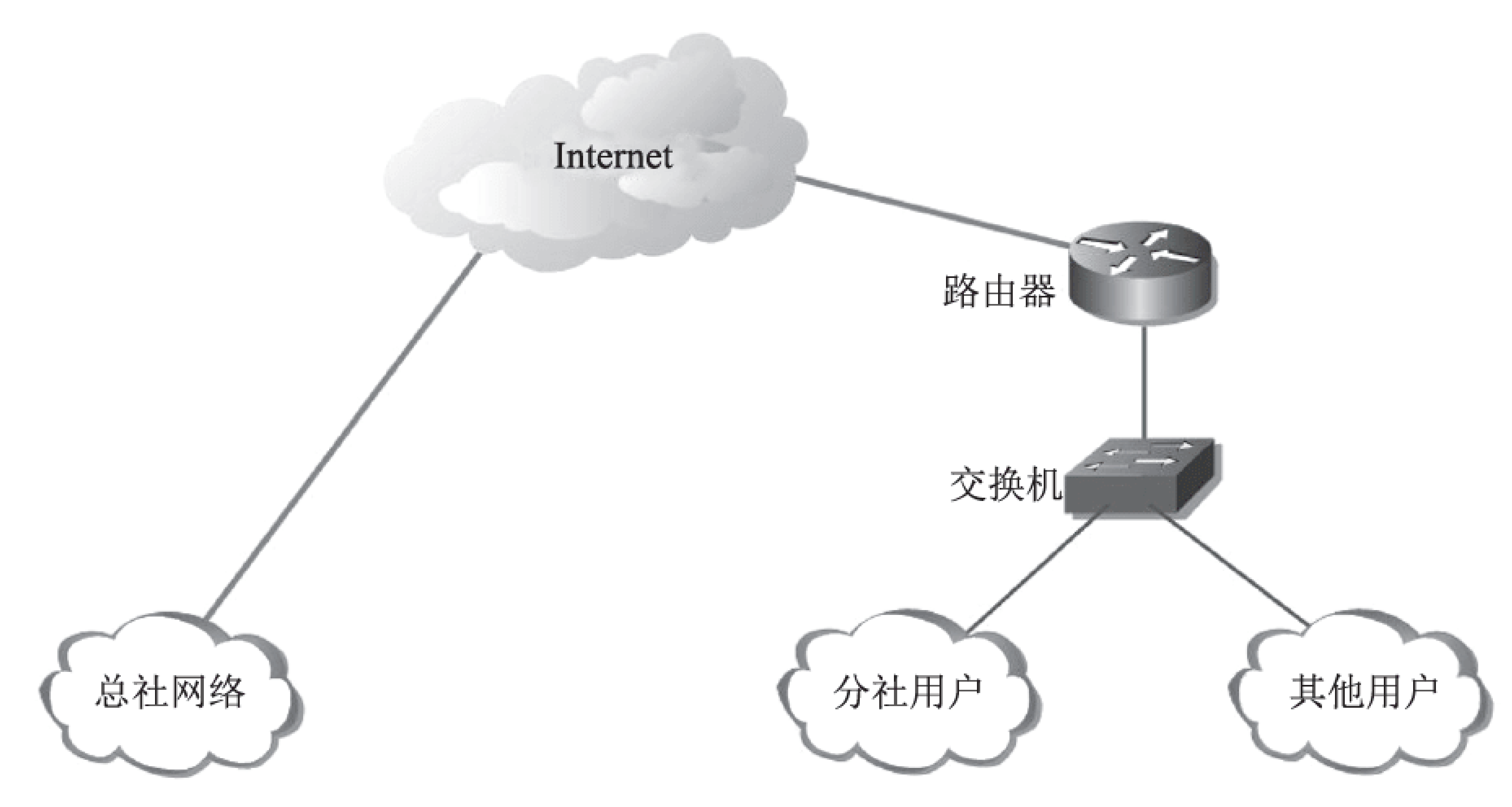


图4-22　分社网络出口结构示意图

解决上面的故障其实也很简单，只要能保证分社用户访问互联网有足够的用户带宽即可。一种方法是可以在分社的网络中，安装部署上网行为的管理设备，严格限制用户传输和工作无关的访问互联网的流量，以保证正常工作的网络流量。第二种方法是把分社用户的出口光纤和图4-22中“其他用户”的出口光纤分开，不要合二为一，而是各用各的。这样分开后，分社用户互联网出口光纤的带宽就不会受到“其他用户”的影响。

4. 总结

SSL VPN采用标准的安全套接层协议对传输中的数据包进行加密，从而在应用层保护了数据的安全性。此协议基于X.509证书，支持多种加密算法。在和IPSec VPN的竞争中，SSL VPN越来越显示出它的优越性。不但配置简单，而且部署容易，使用方便、灵活，特别适合用于满足移动用户在家办公或远程办公的

需求。报业通常在国内外拥有许多分支机构，记者在世界各地捕捉最新的新闻消息。同时，对于报社的编辑记者访问报社内部网络有着大量的需求，SSL VPN的出现可以极大地方便记者移动办公、编发稿件，从而提高报社新闻采编的技术性。

4.5　运维实例：IDS在网络中的部署与配置

随着互联网的高速发展，也产生了各种各样的安全问题。网络中的蠕虫、病毒及垃圾邮件肆意泛滥，木马无孔不入，DDoS攻击越来越常见，黑客攻击行为几乎每时每刻都在发生。如何及时地、准确地发现违反安全策略的事件并及时处理，是广大企业用户迫切需要解决的问题。

IDS(Intrusion Detection System，入侵检测系统)是对防火墙的有效补充，能实时检测网络流量，监控各种网络行为，对违反安全策略的流量及时报警和防护，实现从事前警告、事中防护到事后取证的一体化解决方案。IDS都具有高性能、高安全性、高可靠性和易操作性等特点，具备全面入侵检测、可靠的WEB威胁检测、细粒度流量分析及用户上网行为监测等四大功能，为用户带来了极佳的安全体验。

1. 公司网络结构

网络结构图如图4-23所示。为了确保重要设备的稳定性和冗余性，核心层交换机使用两台Cisco4506，通过Trunk线连接。在接入层使用了多台Cisco3750交换机，图示为了简洁，只画出了两台。在核心交换机上连接有单位重要的服务器，如安全中心、DHCP、E-MAIL和WEB服务器等。单位IP地址的部署，使用的是B类私有172网段的地址。安全中心服务器的IP地址是172.16.2.1/24，DHCP服务器的地址为172.16.10.1/24。

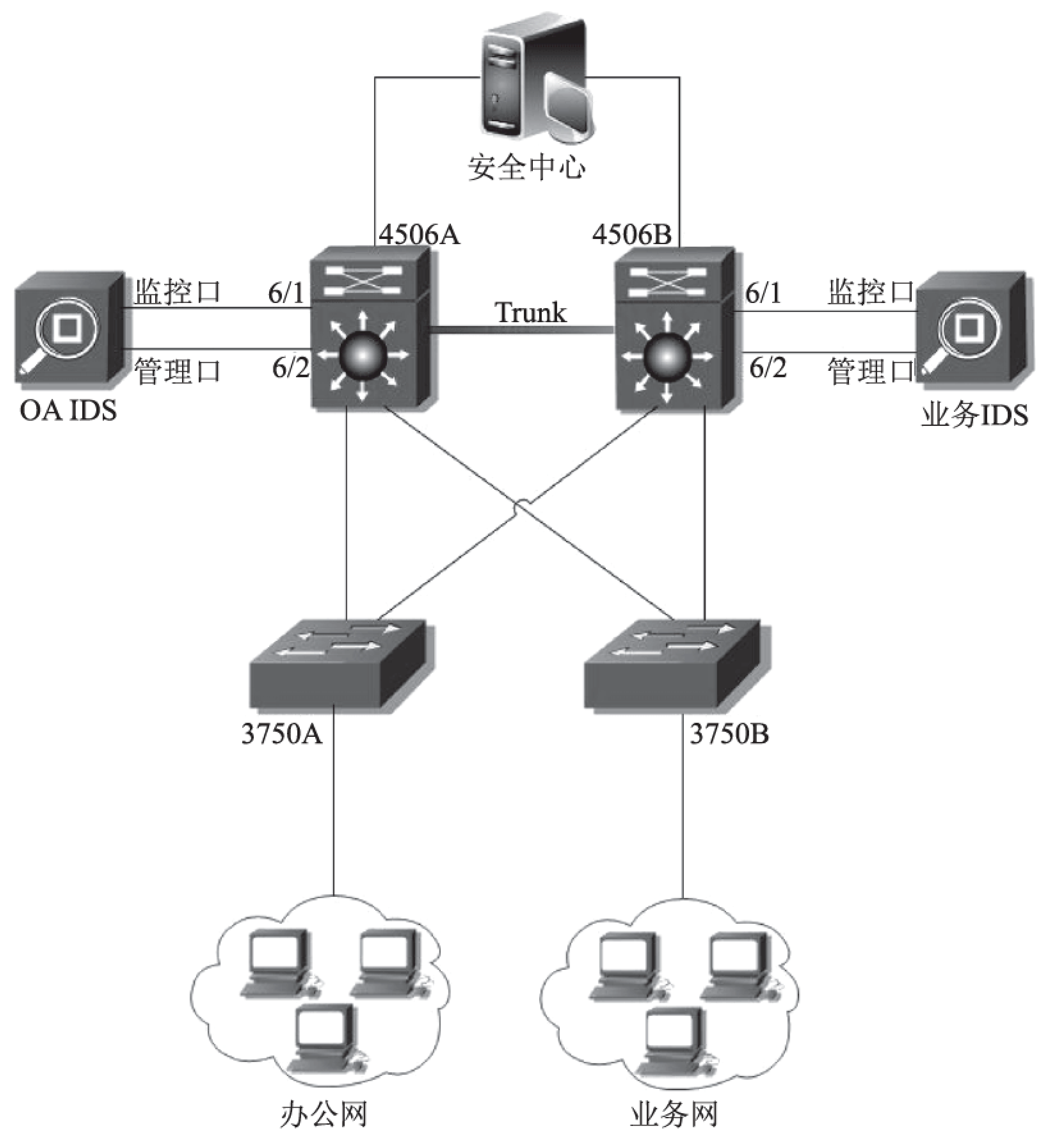


图4-23　网络结构图

2. 网络设备和IDS主要配置

(1)网络设备配置。单位网络主要分为办公网和业务网，业务网所使用VLAN的范围是VLAN 11～VLAN 30，办公网所使用的VLAN范围是VLAN 51～VLAN 90。两个网都是通过两台核心交换机4506交换数据的，但在逻辑上是相互隔离的，只有特定的IP地址才能访问到网络以外的资源。单位的服务器都是直接连接到4506上，所使用的VLAN范围是VLAN 2～VLAN 10。

①在业务网中，根据部门性质的不同，在Cisco4506和Cisco3750上做相应的配置，把它们划分到不同的VLAN中。下面以业务网中VLAN 11的配置为例，列出其相关命令，首先是在Cisco3750B上的配置如下所示：

```
Cisco3750B#VLAN database
Cisco3750B(VLAN)#VLAN 11          //创建VLAN 11
Cisco3750B (config)#interface range gigabitEthernet 1/0/1-24
//对3750上1～24端口同时进行配置
Cisco3750B (config-if-range)# switchport
Cisco3750B (config-if-range)#switchport access VLAN 11
//把3750上1～24端口都划入VLAN 11
```

Cisco4506B上的配置如下所示：

```
Cisco4506B(config)#interface VLAN 11
Cisco4506B(config-if)#ip address 172.16.11.252 255.255.255.0
//创建VLAN 11的SVI接口，并指定IP地址
Cisco4506B(config-if)ip helper-address 172.16.10.1
//配置DHCP中继功能
Cisco4506B(config-if)standby 11 priority 150 preempt
Cisco4506B(config-if)standby 11 preempt
Cisco4506B(config-if)standby 11 ip 172.16.11.254
//配置VLAN 11的HSRP参数
```

②同样在办公网中，也是根据部门性质的不同，把它们划分到不同的VLAN中，也要在Cisco3750A和Cisco4506A上进行和上面相对应的配置。

③网络中的“安全中心”服务器，在连接到网络中时，为了保证它在网络中的冗余性和稳定性，服务器上使用了双网卡，也就是一块网卡连接到4506A，另外一块网卡连接到4506B，两块网卡使用的是同一个IP地址172.16.2.1/24。这样就

可以避免当服务器上的一块网卡故障时，另外一块网卡可以马上由备用状态转换为转发状态，从而不会影响“安全中心”服务器和核心交换机的数据通信。

单位网络中的服务器都是直接连接到核心交换机4506上的，如图4-24所示。所以有关服务器的网络配置，都是在4506上配置的，下面以VLAN 2为例说明它在Cisco4506A上的配置如下所示：

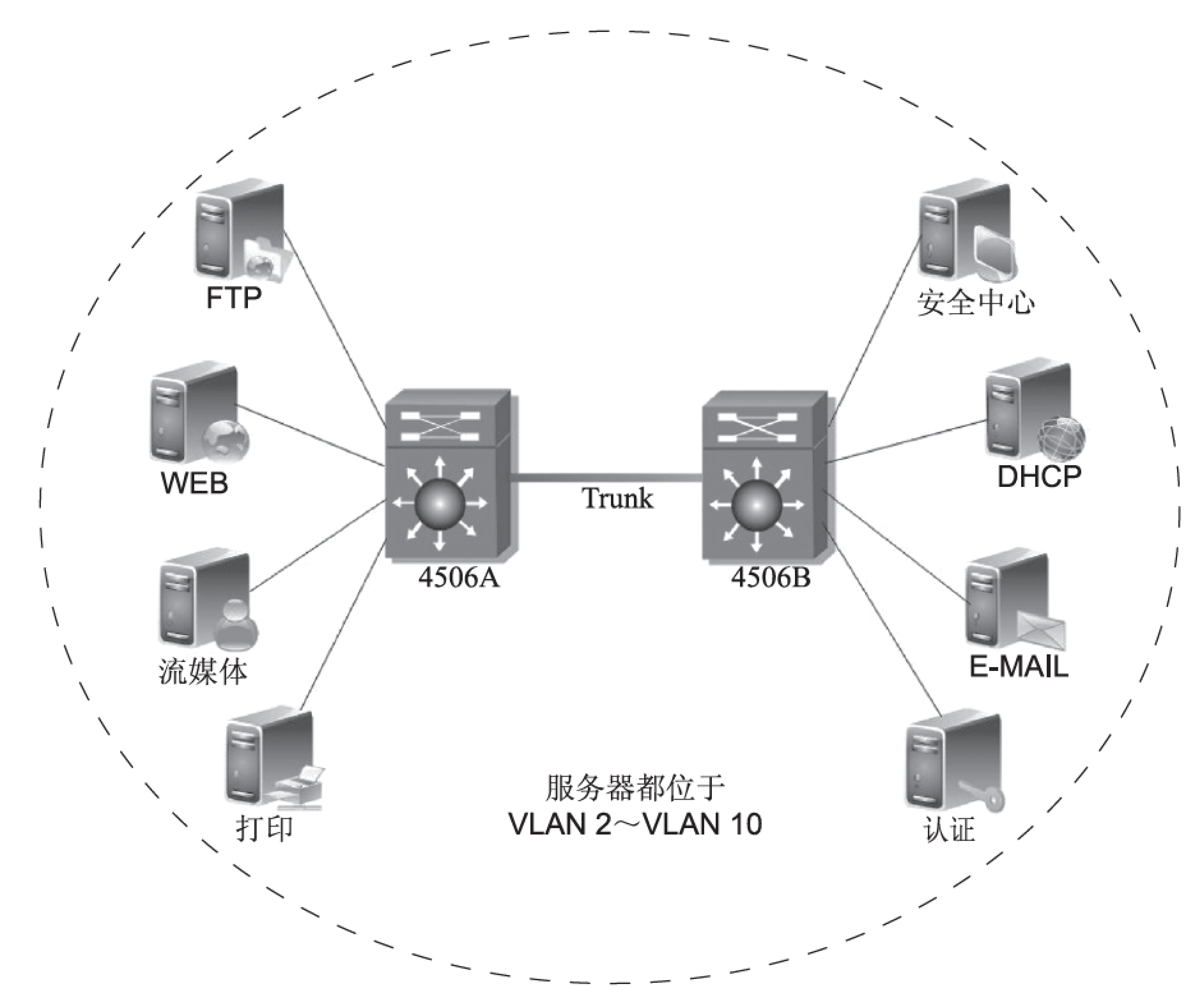


图4-24　服务器在网络中的连接示意图

```
Cisco4506A#vlan database
Cisco4506A(VLAN)#VLAN 2
Cisco4506A (config)#interface range gigabitEthernet 6/2-10
Cisco4506A (config-if-range)# switchport
Cisco4506A (config-if-range)#switchport access VLAN 2
Cisco4506A(config)#interface VLAN 2
```

```
Cisco4506A(config-if)#ip address 172.16.2.252 255.255.255.0
Cisco4506A(config-if)ip helper-address 172.16.10.1
Cisco4506A(config-if)standby 2 priority 150
Cisco4506A(config-if)standby 2 preempt
Cisco4506A(config-if)standby 2 ip 172.16.2.254
```

同样，在Cisco4506B上也会做如上所示相应的配置。

(2)IDS的相关配置。单位IDS的部署，采用的是在两个关键网段(业务网和办公网)实现监控。并利用安全中心集中管理两台入侵检测系统，以达到实时掌握全网的安全状况。业务IDS和办公IDS针对各自网络中数据性质的不同，制定了不同的规则和响应方式，每个IDS分别执行不同的安全策略，实现面向不同对象、不同策略的精细化入侵检测。

①在两个IDS中，不用对“监控口”做任何的设置，它只是接受从两个4506的6/1镜像端口上传输过来的数据，然后IDS对数据进行加工和分析。在4506A和4506B上对镜像口6/1的配置如下所示，首先是在4506A上的配置：

```
Cisco4506A (config)#monitor session 1 source VLAN 11-30 , 2-10 both
Cisco4506A (config)#monitor session 1 destination
interface gigabitEthernet 6/1
```

第一个配置命令意思是指定SPAN的会话号为1，并对VLAN 11～VLAN 30和VLAN 2～VLAN 10中的双向通信数据流进行监控。第二个配置命令的意思是指定Cisco4506A的6/1端口作为SPAN 1会话的目标端口。

同样，在4506B上做如下配置：

```
Cisco4506B (config)#monitor session 2 source VLAN 51 -
90 , 2 - 10 both
```

```
    Cisco4506B (config)#monitor session 2 destination
interface gigabitEthernet 6/1
```

在4506上要想查看某一会话的配置状态及被监听的端口，可以使用命令“Cisco4506A#show monitor session 1”，也可在后面再加上一个“detail”参数，就会显示出更加详细的内容。如果要取消某一SPAN会话，可以使用命令“Cisco4506A (config)# no monitor session 1”。

SPAN(Switched Port Analyzer，交换端口分析仪)，有时也称端口镜像或者端口监控。利用SPAN技术可以把交换机上某些想要被监控端口的数据流复制或镜像一份，发送给连接在监控端口上的IDS。这样IDS就可以对所有的数据进行全面的分析监控。

②对业务IDS和办公IDS的管理和配置都是通过“安全中心”服务器实施的。两台4506都是通过端口6/2和IDS连接，因为从上面的配置中可以看出两台4506端口6/2都划入到了VLAN 2中。

同时，把业务IDS管理口的IP地址配置为172.16.2.2/24，办公IDS管理口IP地址配置为172.16.2.3/24，安全中心的IP地址是172.16.2.1/24。所以两台IDS和安全中心服务器的IP地址都是在同一网段。当管理和配置IDS时，只需在安全中心服务器的浏览器地址栏中输入对应IDS管理口的IP地址，就能进入对应IDS的WEB管理配置界面，然后就能对IDS各个参数进行设定。

3. 结束语

目前，互联网上每天都有成千上万的蠕虫、病毒、木马、垃圾邮件在网络上传播，阻塞甚至中断网络；企业内部员工试图尝试获取未授权的企业内部资源；同时随着安全漏洞不断被发现，入侵者的技巧和破坏能力不断提高，而且入侵者在实施入侵或攻击时往往同时采取多种入侵的手段，以保证入侵的成功几率。这些威胁对企业造成了巨大的损失，而对于上述威胁，传统防火墙和防病毒系统都无法有效地检测。为了弥补防火墙的不足，我们需要利用IDS，实时监控网络资源，精确识别各种入侵攻击，防止入侵造成危害。在检测到入侵攻击时，能够及时报警，动态防御，减少入侵带来的损失。

第5章 虚拟化和IPv6



虚拟化和IPv6曾经是很热的词汇，不过现在逐渐地被大数据所取代。虚拟化技术现在已应用到绝大多数的公司和企业中，也确实给这些单位带来了实实在在的好处。比如服务器虚拟化，原来是单位每上一个应用系统，就需要有一台服务器去支撑，若考虑到双机热备的话，则至少需要部署两台。如果有20个应用系统，双机热备部署，就需要40台服务器，再加上大概5台数据库服务器。这20个应用系统，总共需要45台服务器，按照10台服务器一个机柜，就需要5个机柜。

放置机柜你绝对不能把它放置在办公室那样的环境中，必须放置在专业的机房中。要保证服务器和应用系统24小时无间断地工作，就必须在机房的电力、温湿度、消防和除尘上做好充分的保障，任何一个细小的环节出现问题，都会引起严重的后果。所以一个单位要降低在信息化方面的资金投入，减少应用系统的服务器数量，就成了重中之重。

所以，虚拟化这是就应运而生，服务器虚拟化就是把多台物理服务器的硬件资源进行重新组合，然后进行再分配，它能把多台服务器虚拟成更多或更少数量的虚拟服务器。比如上面的20个应用系统，不使用虚拟化技术，需要45台物理服务器，使用虚拟化技术后，一般用20台物理服务器就能满足要求，可以把20台物理服务器虚拟成45台虚拟服务器，供20个应用系统使用，前后对比一下，使用虚拟化技术，为单位节约了一大半的资金投入，所以说虚拟化技术带来的实惠是实实在在的，它的广泛应用也是大势所趋。

上面说的是服务器虚拟化，这里再说说桌面虚拟化。比如说一个有200名员工的小企业，你需要给每位员工配置一台电脑，价格每台6千元，200台就是120万，若使用桌面虚拟化技术，则每位员工的电脑，就可以用瘦客户机代替，也就相当于每位员工电脑的主机就不需要了，只需在办公桌上放置一台类似显示器的设备，在后台再配置四台高性能的桌面虚拟化服务器，每台服务器按照5万元来算，4台共是20万元，200台瘦客户机，每台2千元，共40万元，使用桌面虚拟化技术总工花销60万元，也就是使用桌面虚拟化技术，现在只需要花60万元，就能实现原来要花120万元才能办到的事，实惠就摆在眼前，新技术何乐而不用。

而使用桌面虚拟化，给系统运维人员也带来了极大的便利。因为员工使用操

作系统，如Win 7、Win XP等，应用软件如Word、Excel等，都是在桌面虚拟化服务器后台生成的，通过网络推送到员工的瘦客户机上，不需要再像以前，需要在每位员工的电脑上安装操作系统和办公软件等，而且系统运维人员在用户出现故障后，主要的运维对象是集中在桌面虚拟化的服务器上，不需要跑来跑去，在员工的电脑上进行维护和操作。这就大大降低了运维人员的人工成本。

IPv6曾经在ICANN(The Internet Corporation for Assigned Names and Numbers，互联网名称与数字地址分配机构)把IPv4地址快分配完的时候，也很火了一段时间。就好比是我们现在使用的身份证号码，因为人口数量的急剧增长，现在的身份证号的位数已不能满足这么多人使用，必须扩充身份证号码的位数，才能满足需要一样。IPv6的产生也是同样道理，而且IPv6的地址数量确实是够多的，号称是把地球上的每粒沙子都能分配一个IPv6地址。

不过现实中，用户对使用IPv6的地址并没有那么迫切，应该是IPv4中的私有地址和NAT技术的作用，一个单位并不需要给每位员工的电脑分配一个全球唯一的IPv4的地址，使用多个IPv4私有地址和NAT技术，也完全可以满足每位员工正常访问互联网，这样就大大延迟了IPv6技术在全球的推广使用。

5.1　运维实例：虚拟化终端防护探讨

虚拟化技术目前在企业中应用越来越广泛，但随之而来的安全问题也越来越引起人们的重视。文章结合虚拟化技术的实际情况，分析了虚拟化应用的安全漏洞，并针对问题提出了多个安全防护措施。解决了当前流行的虚拟化应用在安全方面的薄弱环节。

虚拟化应用不但满足了传统用户的各种需求，更是方便了手机、手持设备用户的使用，随时随地地通过网络连接到单位的虚拟化应用上。但是，虚拟化应用在给用户带来方便的同时，安全问题也接踵而至。安全和易用从来都是一对矛盾体，不能兼得。

终端安全防护的方法有很多，但和虚拟化这一新技术相关的安全防护知识很少，下面将从三个方面对虚拟化安全防护进行探讨研究。

5.2 虚拟化网络部署架构

5.2.1 设备间连接和配置情况

单位虚拟化网络部署结构图，如图5-1所示。为了确保重要设备的稳定性和冗余性，核心层交换机使用两台Cisco6509，通过Trunk线连接。在核心交换机上连接有单位重要的业务应用服务器，如安全中心、DHCP、E-MAIL和WEB服务器等。单位IP地址的部署，使用的是B类私有172网段地址。

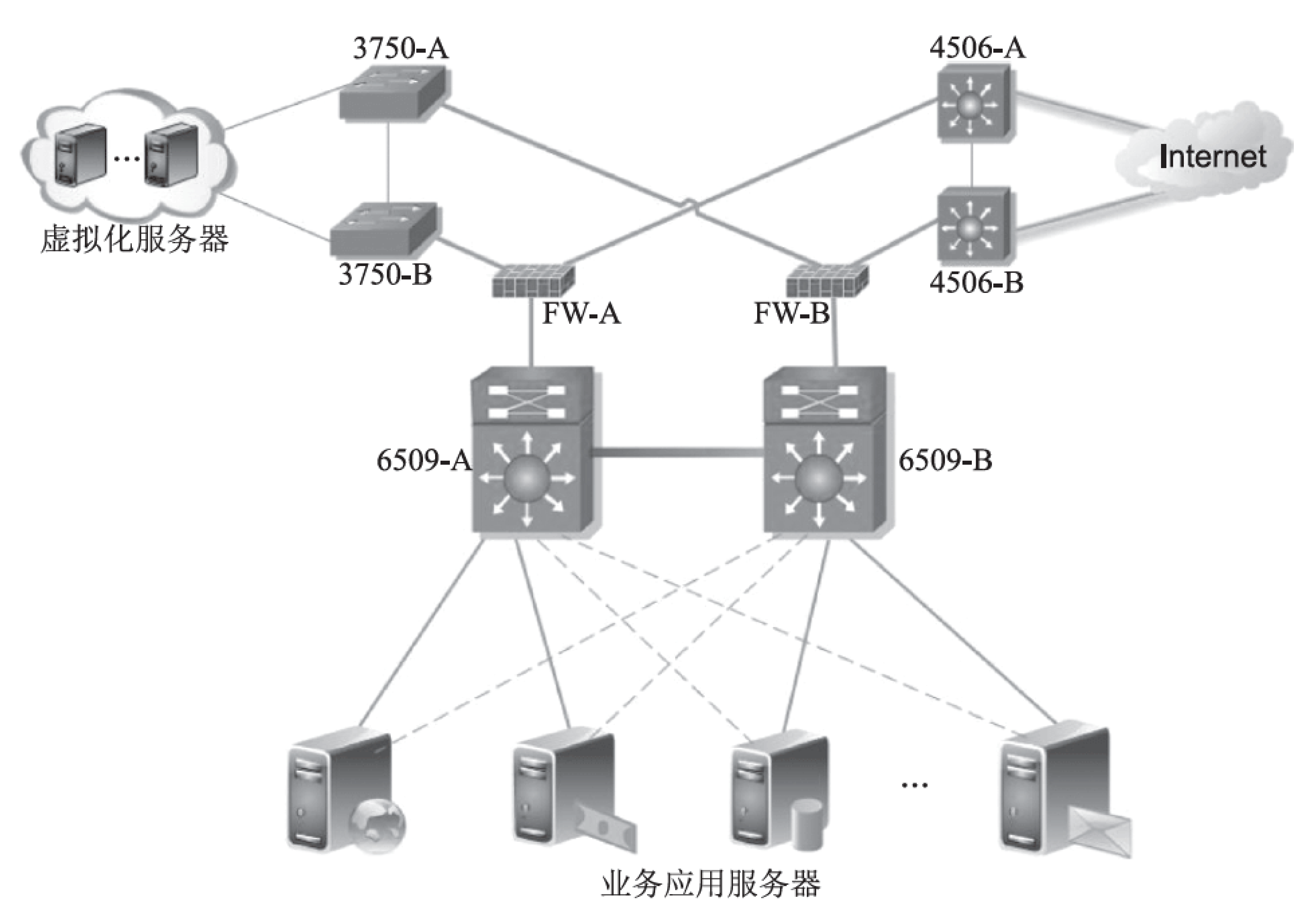


图5-1 虚拟化网络部署架构图

1. 核心设备间连接情况

在图5-1中为了图示的清晰明了没有标出设备间连接的端口号，同时在两台防火墙之间还有一条心跳线，主要作用是检测两台防火墙的运行状态。两台Cisco6509和两台防火墙之间的连接情况，如下所示：

```
    Cisco6509-A GigabitEthernet 1/1 <---> Cisco 6509-B
GigabitEthernet 1/1
    Cisco6509-A GigabitEthernet 3/1 <---> FW-A GigabitEthernet 1
    Cisco6509-B GigabitEthernet 3/1 <---> FW-B GigabitEthernet 1
```

Cisco4506和防火墙之间以及Cisco3750和防火墙之间的连接情况如下所示：

```
    Cisco4506-A GigabitEthernet 3/1 <---> FW-A GigabitEthernet 3
    Cisco4506-B GigabitEthernet 3/1 <---> FW-B GigabitEthernet 3
    Cisco3750-A GigabitEthernet 1/0/1 <---> FW-A GigabitEthernet 2
    Cisco3750-B GigabitEthernet 1/0/1 <---> FW-B GigabitEthernet 2
```

2. 核心交换机配置情况

图5-1中的交换机Cisco6509、Cisco4506和3750都是双机热备部署，运行的热备协议都是HSRP(Hot Standby Router Protocol，热备份路由器协议)，以下是在Cisco6509A上的相关配置情况。其他几台设备上的HSRP配置和在6509A上的配置基本都一样。

Cisco6509A上的配置如下所示：

```
    Cisco6509A#VLAN database
    Cisco6509A(VLAN)#VLAN 2
    Cisco6509A(VLAN)#apply
    Cisco6509A (config)#interface gigabitEthernet 3/1
    Cisco6509A (config-if)# switchport
    Cisco6509A (config-if)#switchport access VLAN 2
```

```
Cisco6509A(config)#int VLAN 2
Cisco6509A(config-if)#ip address 172.16.2.252
255.255.255.0
//创建VLAN 2的SVI接口，并指定IP地址
Cisco6509A(config-if)#no shutdown
Cisco6509A(config-if)standby 2 priority 250 preempt
Cisco6509A(config-if)standby 2 ip 172.16.2.254
//配置VLAN 2的HSRP参数
```

命令“standby 2 priority 250 preempt”中的“priority”是配置HSRP的优先级，2为组序号，它的取值范围为0～255，250为优先级的值，取值范围为0～255，数值越大优先级越高。

优先级将决定一台路由器在HSRP备份组中的状态，优先级最高的路由器将成为活动路由器，其他优先级低的路由器将成为备用路由器。当活动路由器失效后，备用路由器将替代它成为活动路由器。当活动和备用路由器都失效后，其他路由器将参与活动和备用路由器的选举工作。优先级都相同时，接口IP地址高的将成为活动路由器。

5.2.2 虚拟化应用运行过程

从图5-1中可以看出，虚拟化应用位于网络的DMZ区。Cisco6509、Cisco4506、Cisco3750和防火墙设备运行的都是路由模式。Internet上的用户要访问单位的虚拟化应用，数据包首先通过4506交换机，再到防火墙上。在防火墙上配置有相应的安全策略，会根据数据包的源和目的IP地址以及端口号来判断是否对数据包进行路由，允许通过的数据包将会传输到DMZ区的Cisco3750交换机上，最终访问到虚拟化服务器上的业务应用。

互联网上的有些用户，可能还需要通过虚拟化应用访问到单位内部网络上的一些业务应用，这样图5-1中的虚拟化服务器就会作为代理服务器，通过Cisco3750、防火墙和Cisco6509，最终访问到企业内部的业务应用服务器上的资源。从业务应用服务器上返回的数据包也是先到达DMZ区的虚拟化应用服务器上，然后服务器再把数据包返回给Internet上的用户。

5.3　虚拟化客户端安全问题

5.3.1　安全防护五要素

安全是应用的基础。每一个应用都应该从五个方面进行安全加固，如图5-2所示。一是用户身份安全。它能够提供用户名密码、USB-KEY、硬件特征码、数字证书、短信认证中的一种或多种身份认证方式，并可进行多种认证方式之间的“与”、“或”组合认证，保障用户身份接入的可靠性。二是终端安全。应当加强终端设备的病毒、木马防护，及时升级系统的漏洞补丁，检测、拦截和移除病毒、间谍软件。三是传输安全。要使用标准的加密算法保障数据的安全传输。四是应用权限安全。能够针对每个部门、每个用户进行应用、URL级别的授权，并可针对用户终端安全环境、登录时间的不同，进行差别授权和灵活控制。可以采用主从账号绑定技术，对用户登录的账号进行强制指定，防止采用他人账号的越权访问行为。五是审计安全。日志中心能提供详细的报告，作为网络规划的依据，并且具备管理员权限的分级功能，提高管理安全性。



图5-2　安全防护五要素

5.3.2 虚拟化应用安全隐患

企业远程虚拟化应用最普遍的使用方法是，用户用各种终端通过互联网接入到单位的内部网络，最后通过单位的内部网络连接到企业的虚拟化应用上，如图5-3所示。

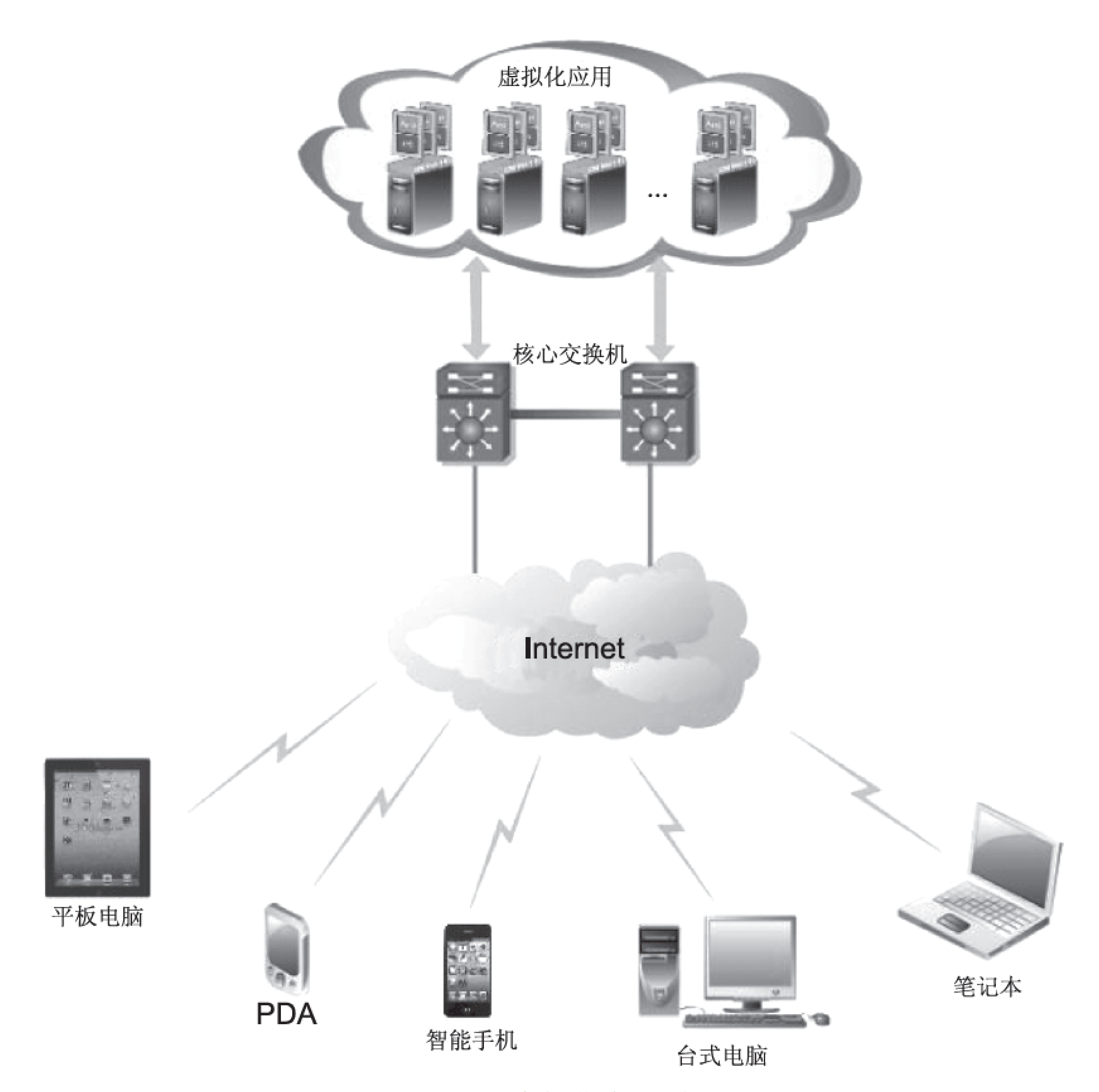


图5-3 远程虚拟化应用原理图

从图5-3中可以看出，接入到虚拟化应用的终端有很多种，只要能接入到Internet就可以访问到企业的虚拟化应用。各种终端的安全防护，可以通过杀毒软件和系统的漏洞、补丁升级进行维护。当前，正流行的Apple和Android系统也会定期发布一些安全补丁，都是为了加固苹果手机、iPad和安卓版手机的终端安全。

但是，访问虚拟化应用的“用户身份安全”不是很好验证。因为要保证用户通过不同终端访问到虚拟化应用，使用台式机上的身份认证方式，不一定能在智能手机或平板电脑上使用。例如，目前广泛使用的USB-Key认证都具备硬件PIN

码保护，PIN 码和硬件构成了用户使用USB-Key 的两个必要因素，即所谓“双因子认证”。用户必须同时取得USB-Key和用户PIN码，才可以登录虚拟化应用系统。即使用户的PIN码被泄漏，只要用户持有的USB-Key不被盗取，合法用户的身份就不会被仿冒；如果用户的USB-Key丢失，若拾获者不知道用户的PIN码，它也无法仿冒访问虚拟化应用系统用户的合法身份。因为目前广泛使用的台式机和笔记本上，都有USB接口，所以USB-Key的认证方式才会得到普遍应用。

现在，具备USB-Key认证的用户就不能用这种认证方式通过智能手机或PDA(Personal Digital Assistant，掌上电脑)访问企业的虚拟化应用，因为这些设备上没有USB接口。所以企业为了方便用户访问虚拟化应用，就开通了“用户名密码+认证码”的认证访问方式，这样用户无论使用什么样的终端都可以访问到虚拟化应用。

但是，使用“用户名密码+认证码”的认证方式属于静态认证，一旦用户名和密码泄露会造成严重的后果。况且认证码也是一种非常简单的认证方式，它的目的是保证登录网站的是人而不是程序，以防止某些人利用程序自动登录网站下载资料，过多占用网络带宽和服务器资源。当用户登录企业虚拟化应用时，系统会以图像的形式显示一个认证码，并要求用户输入这个认证码，二者相符时，用户才能成功登录虚拟化应用系统，否则将提示出错信息。即便这样也不能解决此方式带来的安全隐患，因为非法用户完全可以通过一些专用的破解软件，把密码破译出来。所以，在企业的虚拟化应用上最好不要使用“用户名密码”的认证方式。

5.4　虚拟化客户端安全防护措施

5.4.1　手机动态密码验证

这种认证方式，在国内有的银行已经广泛应用，例如交通银行。它是一种动态的、互动的密码认证方式，即使非法用户盗用了银行用户的银行卡和支付密码，若他没有银行用户的手机也不能完成网上支付，因为动态密码只发送到银行用户本人的手机上。

而且在向银行用户发送动态密码时会包括一个“密码序号”，如图5-4所示的上半部分，是用户进入到银行支付页面的提示。在“动态密码”输入框的后边就有一个提示“密码序号：56”；同样在图5-4的下半部分的黄色显示区域，是银行用户本人手机上收到的动态密码提示信息，在其中也包含有“密码序列：56”，这两个序号的数值必须一致才是真实有效的密码，这就进一步提高了手机动态密码的安全性。



图5-4　手机动态密码应用实例

5.4.2　扩展USB-Key认证使用范围

从表5-1中可以看出，安全性最高的是USB-Key和动态口令认证方式，根据现实情况适用于企业做身份认证的只有动态口令和USB-Key认证。

表5-1　三种常用认证技术比较

程度 / 认证技术	易用性	安全性	可靠性	经济性	接受度
USB-Key	中	高	高	中	中
动态口令	低	高	高	低	低
用户名密码	中	低	中	高	低

1. USB-Key认证特点

(1)带有安全存储空间。USB-Key 具有8 K～128 K 的安全数据存储空间，可以存储数字证书、用户密钥等秘密数据，对该存储空间的读写操作必须通过程序实现，用户无法直接读取，其中用户私钥是不可导出的，杜绝了复制用户数字证书或身份信息的可能性。

(2)硬件实现加密算法。USB-Key 内置微型智能卡处理器，加解密运算在USB-Key 内完成，保证了用户密钥不会出现在计算机内存中，从而杜绝了用户密钥被黑客截取的可能性。一般支持RSA、DES、SSF33 和3DES 算法。采用1024位非对称密钥算法对网上数据进行加密、解密和数字签名，确保网上交易的保密性、真实性、完整性和不可否认性。

(3)使用方便，安全可靠。USB接口已经广泛应用，而且如拇指般大的USB-Key非常方便随身携带，并且密钥和证书不可导出，KEY的硬件不可复制，保证了使用的安全可靠。

2. 扩展USB-Key认证使用范围

相比较而言，USB-Key认证方式性价比高，而且USB接口又有通用性，因此USB-Key认证技术最适合应用推广。由于USB-Key 具有安全可靠、便于携带、使用方便、成本低廉的优点，加上PKI体系完善的数据保护机制，使用USB-Key存储数字证书的认证方式已经成为目前主要的认证模式。

企业用户通过互联网使用智能手机、PDA等没有USB接口的设备，远程登录虚拟化应用时，可以使用USB接口的转接线，把设备上的接口转换成USB接口，就可以继续使用USB-Key的认证方式。

5.4.3　远程安全桌面

访问虚拟化应用的用户，无论是用USB-Key认证方式，还是用“用户名密码”方式登录虚拟化应用系统时，经常会把企业内网中的资源下载到本地电脑中，其中可能会包含有涉及到单位商业安全的信息，这些信息又极易被黑客和不法分子获取，散播到互联网上，对企业带来极坏的影响。而安全桌面技术的应用可以很好地解决这一问题，如图5-5所示。

安全桌面技术可以防止重要数据留存在用户终端而泄露的风险。所有和虚拟化应用服务器发生的访问行为和传输的应用数据都将置于该安全桌面中，此安全桌面中的所有数据均无法存储到本机、无法拷贝到U盘等外设设备、无法通过局域网/互联网外发，任何方式都无法将数据从安全桌面内泄漏出去。当用户关闭安全桌面后，其中的所有数据将一并销毁，从而彻底保障重要数据被终端访问时

的高安全性。

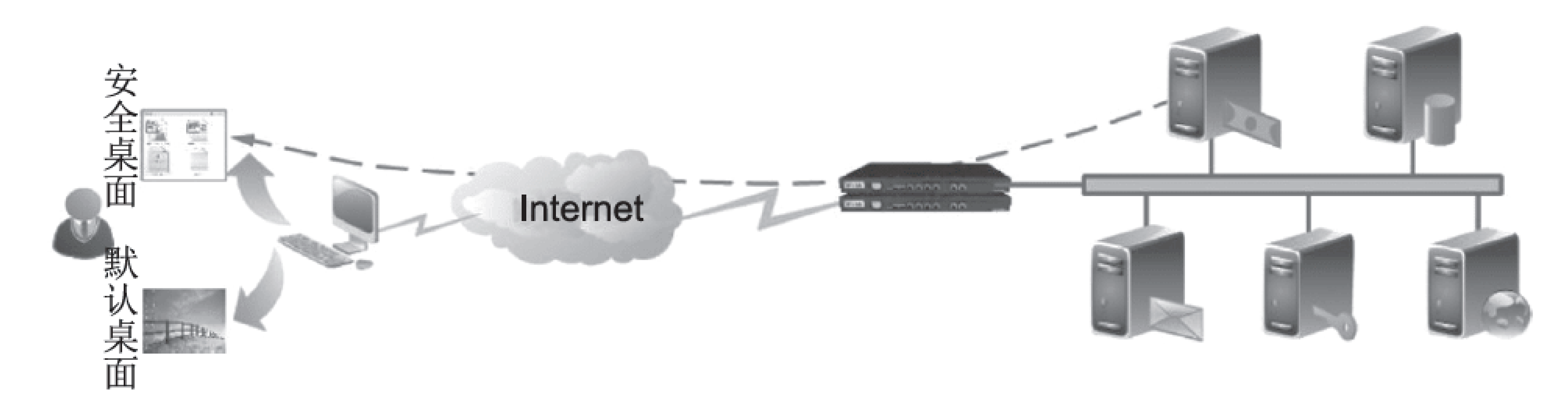


图5-5　安全桌面应用原理图

5.4.4　DMZ区部署七层防火墙

从图5-1中可以看出，互联网上的用户访问单位内部的虚拟化应用的所有数据，都必须通过两台防火墙设备FW-A和FW-B，所以防火墙设备性能的优劣，将会对虚拟化应用的安全性起到决定性作用。

1. 传统防火墙的劣势

目前广泛使用的传统型防火墙主要是基于一种重要的理论假设来进行安全防护的。这种理论认为如果防火墙拒绝某类数据包的通过，则认为它一定是安全的，因为这些包已经被丢弃。但防火墙并不保证准许通过的数据包是安全的，它无法判断一个正常的服务的数据包和一个恶意的数据包有什么不同。传统防火墙也无法提供基于应用和用户的，从第三层到第七层的一体化访问策略控制，黑客常常通过穿透合法的80端口，就可以轻松地让防火墙的安全控制策略变成“聋子和瞎子”。此外，它也无法提供基于应用的流量分析和报表展示，无法帮助用户了解当前网络边界的现状。而且，当前的安全威胁已不再是单一的类型。通常一个完整的入侵行为包含了多种技术手段，如漏洞利用、WEB入侵、木马后门、恶意网站等，如果将这些安全威胁割裂的进行处理和分析，系统的防范短板依然存在。

2. 七层防火墙的优势

七层防火墙加强了允许通过防火墙的数据包的安全性，因为网络安全的真实需求是，既要保证网络安全，也必须保证应用的正常运行。它主要是基于应用层开发的新一代防火墙，与传统防火墙相比它可以针对丰富的应用提供完整的、可

视化的内容安全保护方案。解决了传统安全设备在应用可视化、应用管控、应用防护处理方面的巨大不足，并且满足了同时开启所有功能后性能不会大幅下降的要求。它既满足了普遍互联网边界行为管控的要求，同时还满足了在内网数据中心和广域网边界的部署要求，可以识别和控制丰富的内网应用。

在图5-1所示的网络中部署七层防火墙后，可以识别出Internet上访问虚拟化的各种应用及其应用动作，识别出用户IP地址对应的多种信息，并建立组织的用户分组结构，这将会大大提高互联网用户访问企业虚拟化应用的安全性。

5.5　总结

通过互联网实现的各种应用，在安全上都是相对的。尤其是虚拟化技术的广泛应用，虽然它降低了系统操作代价，改进了硬件资源利用率，以及在灵活性方面扮演着越来越重要的角色。但是，虚拟化技术本身不仅面临着传统网络已有的安全威胁，还面临着自身引入的安全问题。这就需要企业在部署虚拟化应用时，采取灵活、多样的安全防护措施。

5.6　运维实例：搭建IPv6网络环境

从事计算机网络工作，是万万不能少了各种各样的实践操作。但现实中真实网络环境的稀缺，限制了很多想深入学习网络知识的同志。更别说在现实的IPv6网络环境中学习IPv6知识了。本文就是通过使用DynamipsGUI和VMware两个软件，为那些想深入学习IPv6知识的同志，搭建起几乎和现实IPv6网络一样的实验环境。可以随意大胆地在搭建起来的网络环境中进行各种各样的测试和操作，能够很好地提高学习IPv6知识的效率。而且本文中使用的软件在网上都可以找到，在电脑上安装完软件后，完全可以对照下面的步骤一步一步把IPv6的网络环境搭建成功。

1. 网络结构拓扑图和所使用的软件

(1)网络拓扑介绍。如图5-6所示，是搭建的纯IPv6网络环境。最终要实现的功能是从电脑PC上，通过路由器，能ping通服务器Server。反之，也要实现从Server上ping通电脑PC。关于图5-6中具体的参数配置，会在下面进行详细的介绍。

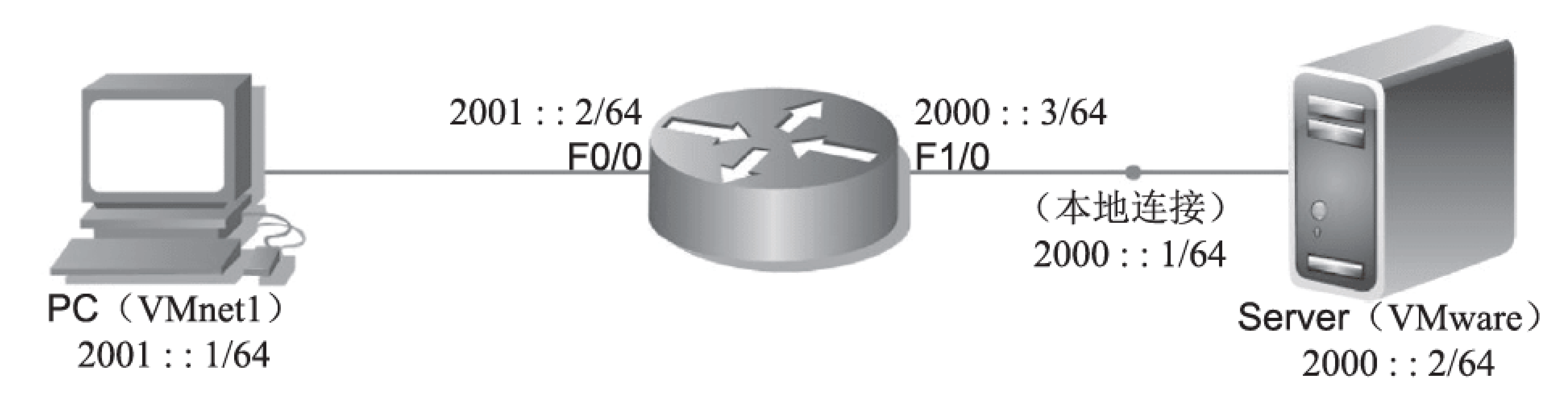


图5-6　网络结构拓扑图

(2)使用软件介绍。图5-6网络环境的搭建都是在一台装有Win 7操作系统电脑上完成的。也就是说在单台电脑上，通过使用软件搭建起了和现实IPv6环境一样的网络。在Win 7操作系统中主要安装了两个软件，一个是DynamipsGUI，版本为2.8；另一个软件为VMware，版本为7.1.3 build-324285，而且在VMware的虚拟机中安装的还是Win 7的操作系统。因为Win 7对IPv6的支持比较好，所以就没有选择在VMware中安装Windows XP系统。

(3)有关上面两个软件的安装和使用，在网上有很多相关的文章，在此就不再一一介绍。只是在虚拟机VMware中安装Win 7系统时可能要注意的事项多一些。

2. DynamipsGUI中的配置步骤

(1)在VMware中安装完Win 7操作系统后，就会在本地电脑(图5-6中的PC)的“控制面板”→“网络和Internet”→“网络连接”中出现两个VMware Network Adapter连接，“VMnet1”和“VMnet8”。因为本实例中只会用到“VMnet1”和“本地连接”，所以就在网络连接“VMnet8”上单击右键，选择“禁用”后就变成了如图5-7所示的灰色的不可用状态。

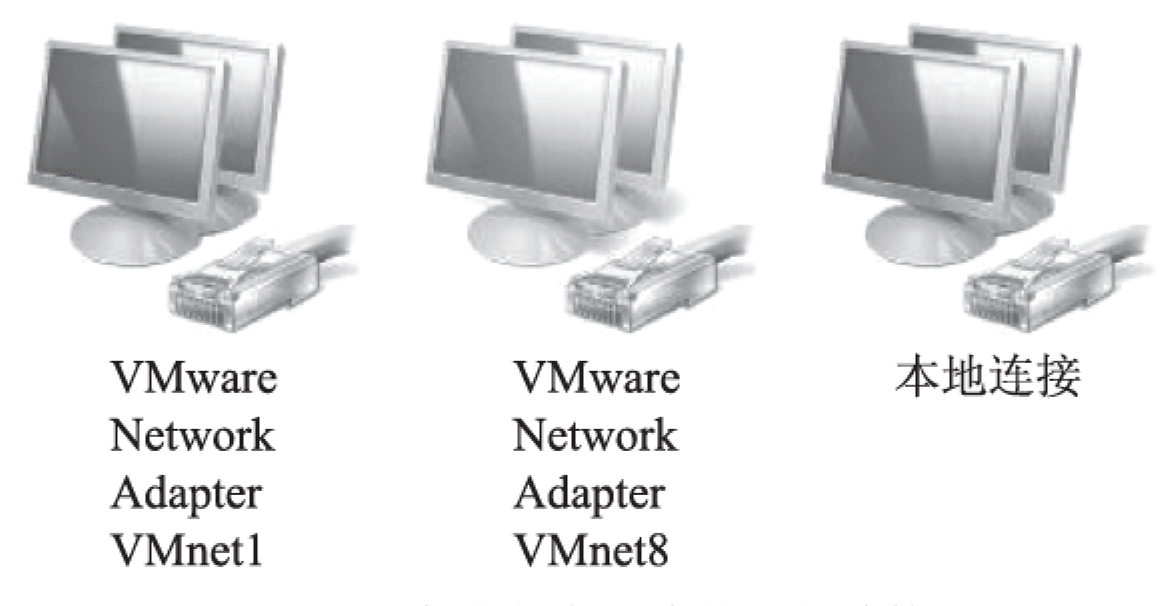


图5-7　本地电脑PC中的网络连接

(2)打开DynamipsGUI 2.8，对照图5-8所示，选择好各个参数：

在“路由器个数”中选择1；

在“设备类型”中选择2600；在“2600”一栏中的各个参数对照图5-8选择。

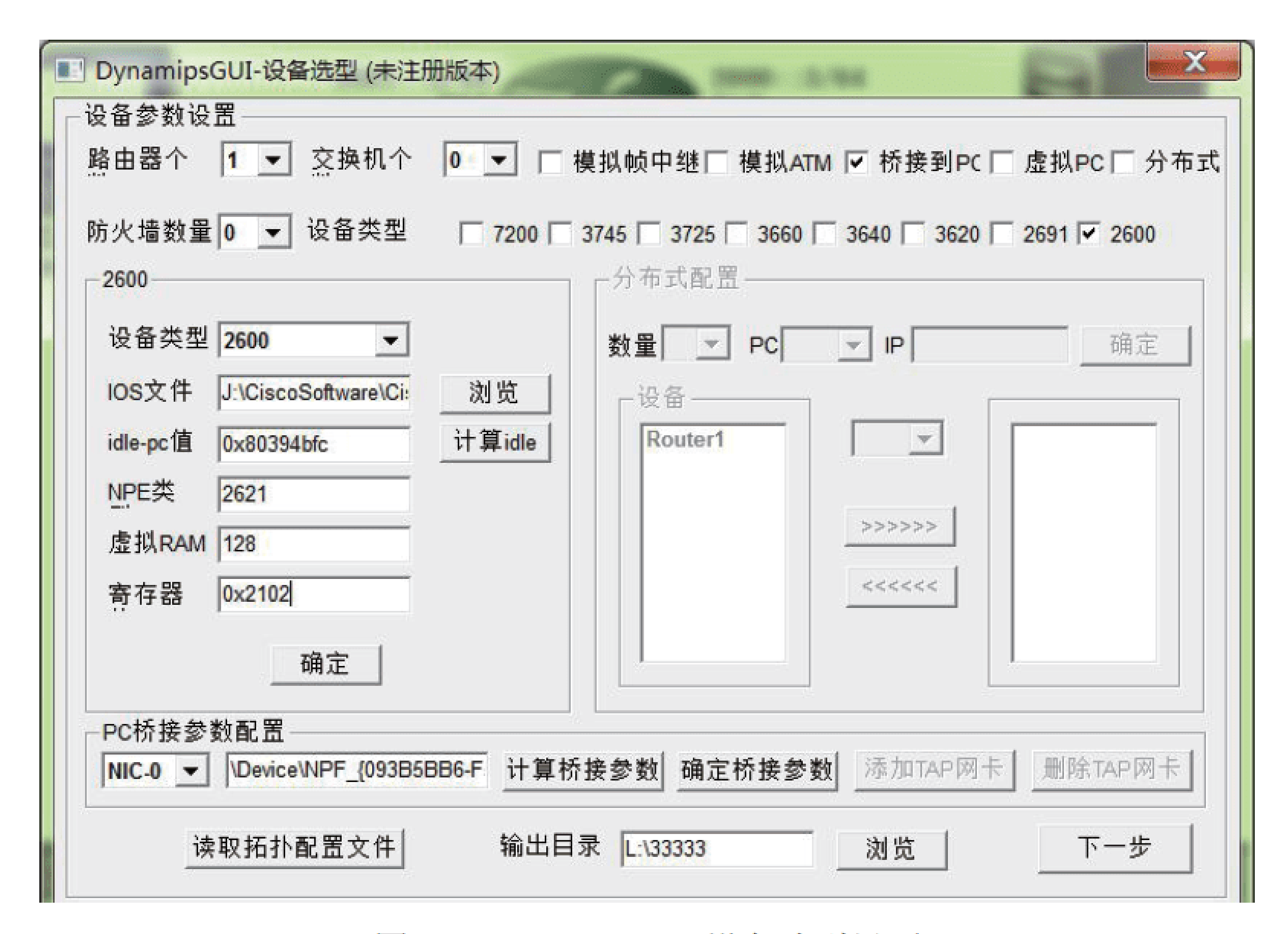


图5-8　DynamipsGUI设备选型界面

在“IOS文件”中使用的是c2600-ik9o3s3-mz.123-13a.BIN，当然也可以使用其他的IOS，只要能保证它支持IPv6的各个功能即可。此处还有一个“idle-pc值”，只要选择好IOS，单击“计算idle”就可以计算出它的值，具体的方法网上都有，不再一一陈述。

在“PC桥接参数配置”中，要计算“VMnet1”和“本地连接”二者的桥接参数。单击“计算桥接参数”按钮，就可得出两个网络连接的桥接参数：

NIC_0(对应图5-7中的“本地连接”)的桥接参数为“\Device\NPF_{093B5BB6-F57D-4210-8BAF-6F98D3237BA5}”。

NIC_1(对应图5-7中的“VMware Network Adapter VMnet1”)的桥接参数为“\Device\NPF_{A0002202-4768-4522-91CF-455D8AFB68A3}”。选择好两个桥接参数后单击“确定桥接参数”。

(3)在图5-8中设置好各个参数后，单击“下一步”进入到图5-9所示的界面。这里主要是选择路由器2621使用的模块类型，对照图5-9所示选择好后点击“确定Router1配置”，再单击“下一步”。



图5-9　DynamipsGUI模块设置界面

(4)进入到“Dynamips-连接设置”界面，如图5-10所示。在此要建立了两个连接，“Router1 F0/0 <----> XPC P0/1”和“Router1 F1/0 <----> XPC P0/0”。这里有几个关键点：两个连接中的Router1 F0/0端口和F1/0端口，就是图5-6所示的两个路由器端口；XPC P0/0接口就是图5-6中的“本地连接”的接口，也就是图5-7中的“本地连接”；XPC P0/1接口就是图5-6中的“PC(VMnet1)”的接口，也就是图5-7中的“VMware Network Adapter VMnet1”网络连接。



图5-10　DynamipsGUI连接设置界面

在图5-10中建立好连接后，再单击“生成.BAT文件”(此按钮在图5-10中没有截出，位于右下方)按钮，即可在设定好的目录下生成可执行文件“Router1.

bat”。在文件“Router1.bat”上单击右键选择“编辑”，就会显示出文件的内容，如下所示：

```
REM ----------Created by Xiaofan----------
@echo off
title Router1-----Created by Xiaofan
mkdir Router1
cd Router1
:reload
..\dynamips-wxp.exe -T 2001 -P 2600 -r 128 -t 2621 -c 0x2102 -p 0:CISCO2600-MB-2FE -p 1:NM-1FE-TX -s 0:0:gen_eth:"\Device\NPF_{A0002202-4768-4522-91CF-455D8AFB68A3}" -s 1:0:gen_eth:"\Device\NPF_{093B5BB6-F57D-4210-8BAF-6F98D3237BA5}" ..\c2600-ik9o3s3-mz.123-13a.BIN --idle-pc=0x80394bfc
goto reload
```

综上所述，图5-6中所示拓扑图的内部连接情况为：

```
Router F0/0<---->VMnet1<---->{A0002202-4768-4522-91CF-455D8AFB68A3}(图5-8中计算得出的桥接参数)<---->NIC_1(图5-8中所示的参数)<---->XPC P0/1(图5-10中所示的设备接口)；
Router F1/0<---->本地连接<---->{093B5BB6-F57D-4210-8BAF-6F98D3237BA5}<---->NIC_0<---->XPC P0/0。
```

3. 在VMware虚拟机中的配置

打开VMware虚拟机后，再启动其中的Win 7操作系统，启动完成后，选

择“VM”菜单中的“Settings”选项，就会出现如图5-11所示的配置界面。在“Hardware”页面中，选择“Network Adapter”选项，然后在页面右边的“Network connection”中选择“Bridged”选项。最后单击“OK”按钮。然后，在VMware虚拟机中再重新启动Win 7操作系统。

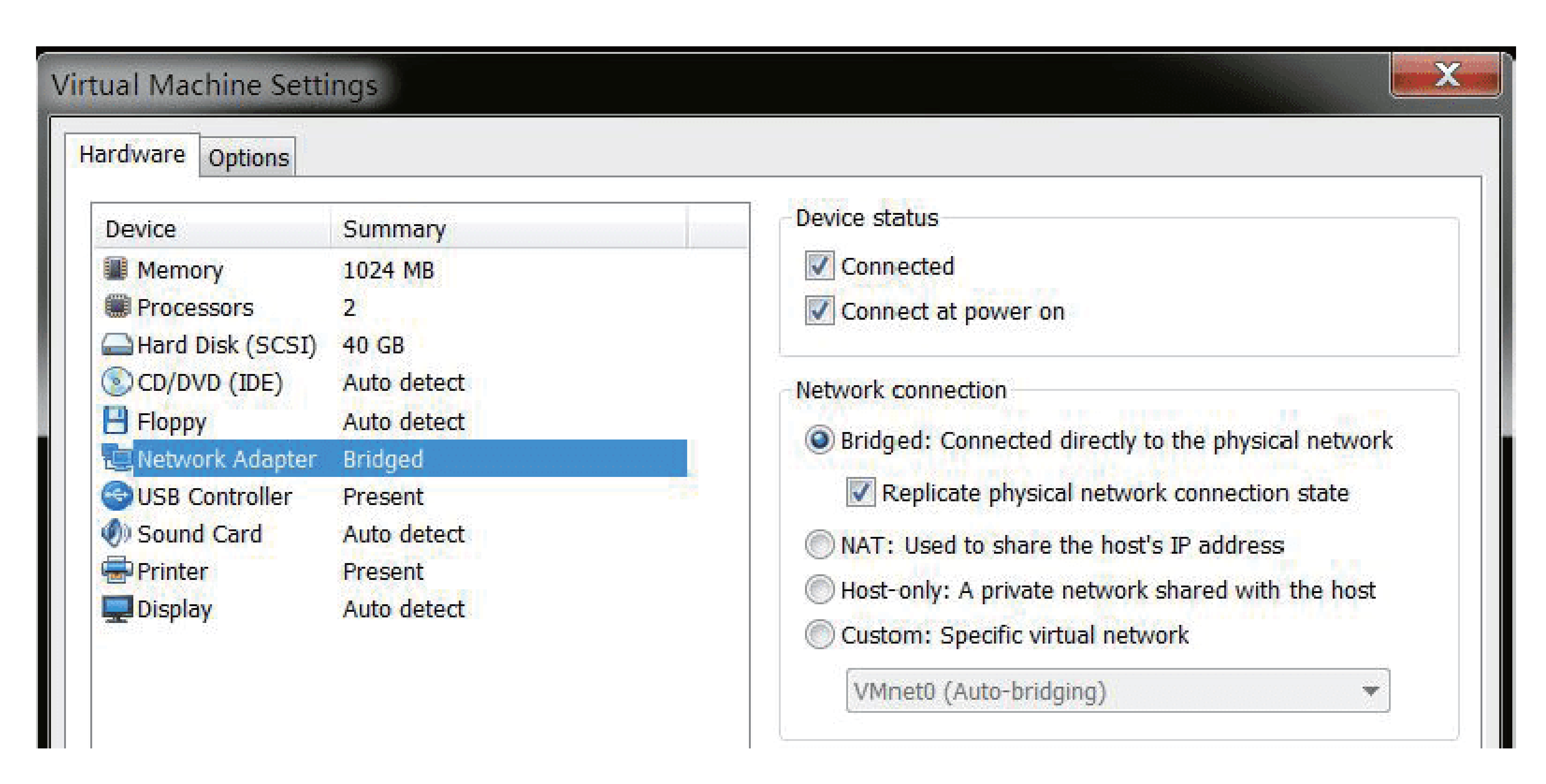


图5-11 VMware网络适配器设置界面

虚拟机中的Win 7操作系统，就相当于图5-6中的“Server”服务器。在虚拟机中安装完Win 7系统后，在其中的“控制面板”→“网络和Internet”→“网络连接”中会自动生成一个虚拟的网络连接。

在图5-11中，选择“Bridged”桥接模式后，就相当于把图5-6中的“本地连接”网卡和“Server(VMware)”上自动生成的虚拟网卡连接到了同一个网段中。这样图5-6中的“Server(VMware)”也就和路由器Router的F1/0位于同一个网段中。

4. 终端和路由器上网络参数配置

要实现图5-6中PC和Server之见的互联互通，就必须在路由器、PC和Server上进行相应的网络配置。

(1)终端网络参数配置。其中Server上IPv6地址的配置，如图5-12所示，直接在虚拟机的Win7操作系统中的“Internet协议版本6(TCP/IPv6)属性”配置，地址为2000::2/64。同理，图5-7中“VMware Network Adapter VMnet1”和“本地连接”两个连接的IPv6参数配置，也和在图5-12中配置的类似。PC(VMnet1)的IPv6地址为2001::1/64，“本地连接”的IPv6地址为2000::1/64。

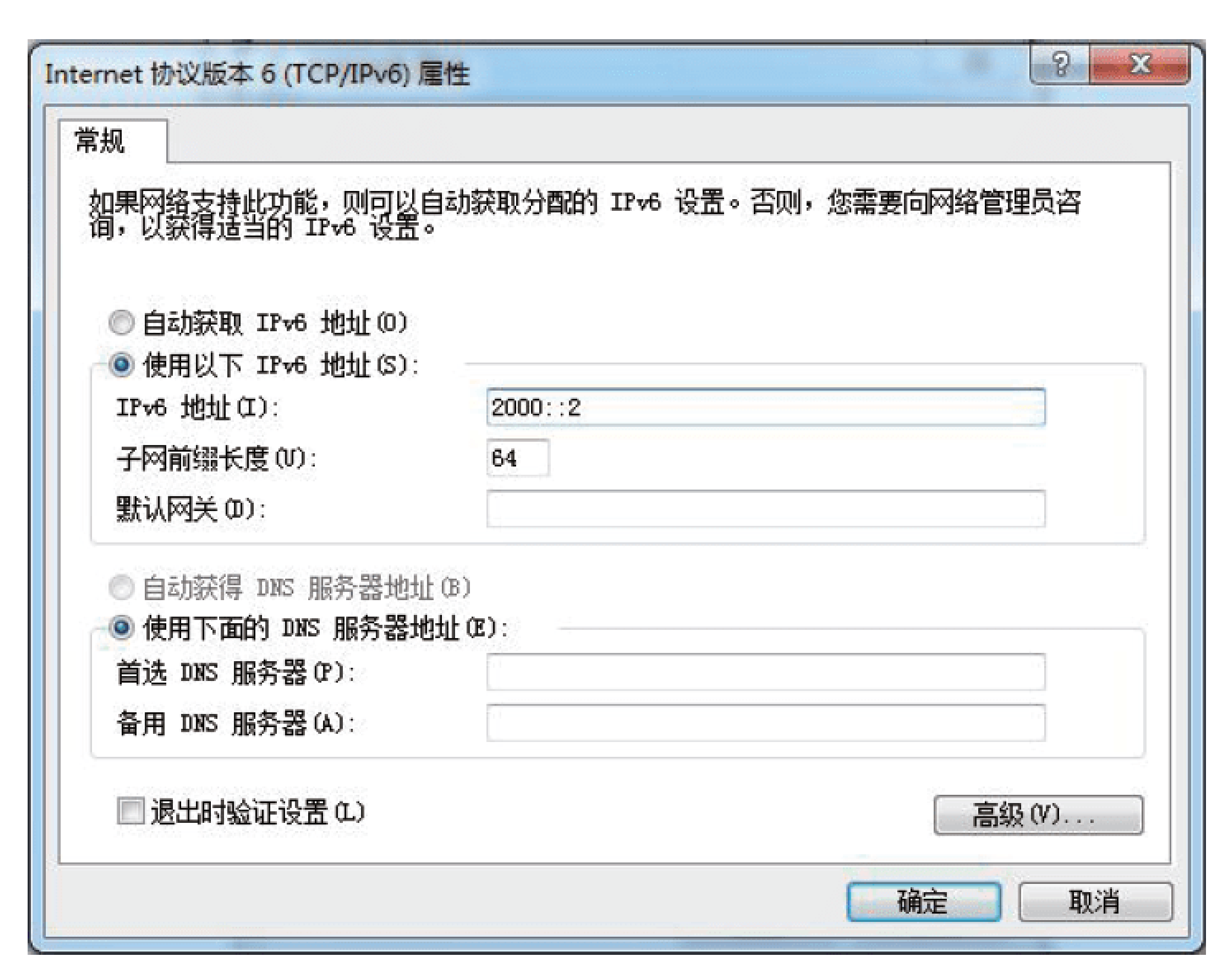


图5-12　在VMware的Win 7系统中配置IPv6地址

(2)路由器上网络参数配置。主要包括三个方面的配置：一是启用Router的IPv6路由，命令为“Router(config)#ipv6 unicast-routing”；二是在接口F0/0上配置IPv6地址，命令如下所示：

```
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001::2/64
```

上面的命令也表示端口FastEthernet0/0位于IPv6的子网2001::/64中。三是在接口F1/0上配置IPv6地址，命令如下所示：

```
interface FastEthernet1/0
 no ip address
```

```
duplex auto
speed auto
ipv6 address 2000::3/64
```

同样，上面的命令也表示端口FastEthernet1/0位于IPv6的子网2000::/64中。配置完成后可以使用如下所示命令查看配置结果：

```
Router#show ipv6 interface brief
FastEthernet0/0             [up/up]
FE80::CA00:17FF:FE94:0
2001::2
FastEthernet1/0             [up/up]
FE80::CA00:17FF:FE94:10
2000::3
```

上面输出中的“[up/up]”表示端口的物理状态和协议状态都是打开的。同时，在每个端口上都会自动生成一个“本地链路”地址，如FastEthernet 0/0端口上的“FE80::CA00:17FF:FE94:0”地址。

5. 网络环境运行和测试

(1)在PC(VMnet1)端测试。在图5-6的PC本机的Win 7系统中打开一“命令行CMD”窗口。在其中执行命令“ping -S 2001::1 2000::2”得到如下所示的输出结果：

```
C:\Users\Administrator>ping -S 2001::1 2000::2
正在 Ping 2000::2 从 2001::1 具有 32 字节的数据:
来自 2000::2 的回复: 时间=371ms
```

```
来自 2000::2 的回复: 时间=5ms
来自 2000::2 的回复: 时间=215ms
来自 2000::2 的回复: 时间=5ms
2000::2 的 Ping 统计信息:
数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
最短 = 5ms，最长 = 371ms，平均 = 149ms
```

注意：上面的ping命令中使用了一个“-S”的参数，后面紧跟的“2001::1”的地址，是VMnet1的IPv6地址，命令最后一个地址“2000::2”才是要ping的目标地址。Win 7系统对ping命令中“-S”参数的解释为“要使用的源地址”，也就是指定ping的数据包从网卡VMnet1发送出去，而不是从其他的网卡把数据传输出去。为了追踪ping数据包的路径，再在“命令行CMD”中执行命令“tracert -S 2001::1 2000::2”，得到如下所示的输出结果：

```
C:\Users\Administrator>tracert -S 2001::1 2000::2
通过最多 30 个跃点跟踪
到 Server [2000::2] 的路由:
  1     5 ms     2 ms     2 ms  2001::2
  2     4 ms     4 ms     5 ms  Server [2000::2]
跟踪完成。
```

从上面的输出结果可以看出，命令“ping -S 2001::1 2000::2”的数据包的传输路径确实是通过路由器Router，再到达Server的。其中，Win 7系统对tracert命令中“-S”参数的解释为“要使用的源地址(仅适用于 IPv6)”。若是在ping的命令中不使用“-S”的参数，ping命令也能执行成功，但它传输的路径就不通过路

由器，而是从“本地连接”的网卡上直接把数据包发送出去，然后到达Server。

为了验证上面的推断，在“命令行CMD”中执行命令“tracert 2000::2”，它的输出和执行命令“tracert -S 2001::1 2000::2”的输出结果是不一致的，这也就进一步说明了参数“-S”的用途，如下所示：

```
C:\Users\Administrator>tracert 2000::2
通过最多 30 个跃点跟踪
到 Server [2000::2] 的路由:
  1    <1 毫秒   <1 毫秒   <1 毫秒 Server [2000::2]
跟踪完成。
```

(2)在Server(VMware)端测试。同样也可以在服务器端进行测试，在虚拟机VMware中的Win 7系统的“命令行CMD”中，执行如下命令：

```
C:\Users\Server>ping 2001::1
正在 Ping 2001::1 具有 32 字节的数据:
来自 2001::1 的回复: 时间=255ms
来自 2001::1 的回复: 时间=5ms
来自 2001::1 的回复: 时间=5ms
来自 2001::1 的回复: 时间=4ms
2001::1 的 Ping 统计信息:
数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
最短 = 4ms，最长 = 255ms，平均 = 67ms
```

从上面的输出结果可以看出，从服务器端到PC端的网络是通的。为了进一步验证ping数据包的传输路径，再在“命令行CMD”中执行如下命令：

```
C:\Users\Server>tracert 2001::1
通过最多 30 个跃点跟踪到 2001::1 的路由
  1      2 ms      2 ms      1 ms   2000::3
  2      7 ms     94 ms     20 ms   2001::1
跟踪完成。
```

从上面的输出结果可以看出，从Server端发出的ping数据包确实是通过路由器Router，最后再到达PC的。

(3)在Web服务器中的测试。为了进一步验证网络环境的可用性，在图5-6的PC(VMnet1)端的Win 7系统中安装了Xampp软件包，此软件中包含有Tomcat的Web服务器，在XAMPP的控制面板中可以直接启用Web服务器，如图5-13所示，是在控制面板中启用了Tomcat服务器的状态。其中Tomcat使用的端口号共有3个：8005、8009和8080。启用WEB服务器后在PC(VMnet1)端的Win 7系统中的浏览器地址栏中输入地址“http://[2001::1]:8080”就可以进入到Tomcat服务器的欢迎界面。



图5-13　XAMPP控制面板图

为了验证图5-6中的IPv6的网络状况，可以在图5-6中的Server端，也就是在虚拟机VMware中的Win 7系统的浏览器地址栏中输入地址“http://

[2001::1]:8080”，回车后也能进入到Tomcat服务器的欢迎界面，如图5-14所示。注意图5-14中浏览器地址栏中的地址为IPv6的地址。

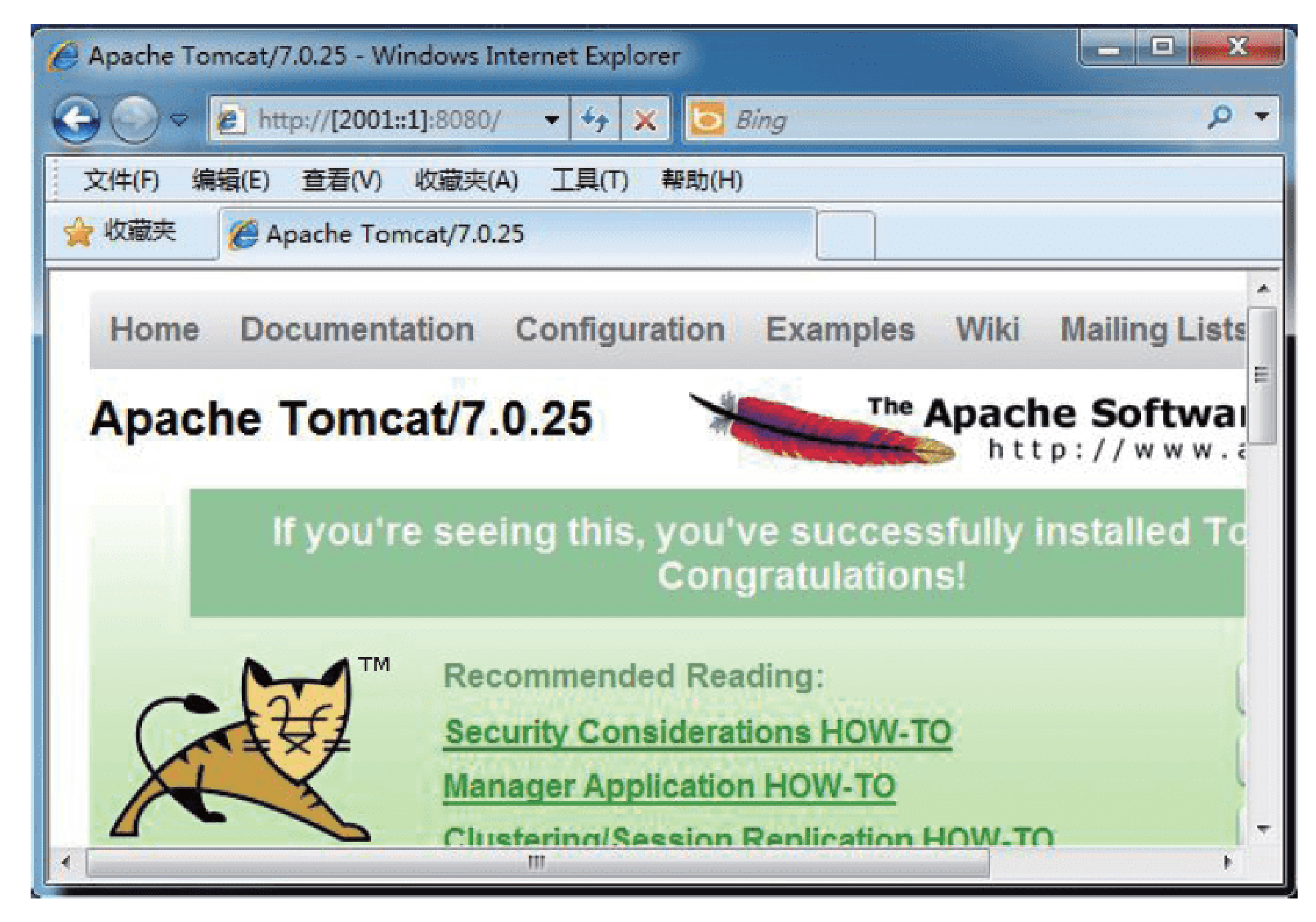


图5-14 在VMware的Win 7系统中访问本机PC上的IPv6 WEB服务器

在IPv4中，对于一个URL地址，当需要通过直接使用“IP地址+端口号”的方式来访问时，可以表示成“http://202.121.23.11:8080”。但是如果IPv6地址中含有“:”，为了避免歧义，在URL地址含有IPv6地址时，用“[]”将IPv6地址包含起来。

6. 总结

(1)如图5-6所示的IPv6的网络环境，只是一个非常简单的网络。读者可以根据自己的实际情况把它复杂化，以满足各种各样的网络测试需求。利用DynamipsGUI软件是可以很方便地把几台或多台路由器、交换机和防火墙互联起来，但要用它模拟现实网络中复杂的客户端和服务器端就有些难度。图5-6网络结构虽然简单，也只是把基本的框架搭建起来，但它搭建的客户端和服务器端已经很接近现实了，实现了在上面“5”的第3点中进行WEB服务测试的需求。另外，也可以把图5-6中的一台路由器变成三台、五台，或更多的路由器互联，在它们上面运行RIP、OSPF或者EIGRP协议，以便进行更复杂的网络实验。

(2)本例中各个设备之间的内在逻辑连接关系比较复杂，但只要对照步骤一步步做下来就能明白其中的原理。主要是因为DynamipsGUI和VMware两个软件

和本地电脑建立的连接都是虚拟连接，不像现实中电脑都是通过网线连接到交换机上，看得见摸得着比较容易理解。所以一定要搞清楚两个软件具备的功能和使用方法，这样才好理解使用它们搭建起来的网络环境。

(3)实践是检验网络搭建和配置是否正确的唯一标准。从我自己开始参加CCNA培训，到后期的CCIE的培训，几乎每一堂课都有实践操作，都有实验。甚至在CCIE的培训中，绝大部分的时间和精力放在“CCIE集训营”、“CCIE LAB实验室”等这些实实在在的实验上。这是因为我们学到的每一个知识点，最终都要在实践中验证，通过做实验来说明它是正确的还是错误的。

包括平时在书本上，或网上看到一些知识点，可能在原理上都能明白，知道它们运行的机制和过程。但即使是这样，也只有通过把这些知识点涉及到的一些命令在交换机、路由器等设备上操作一遍，看看它们到底符合不符合书上所讲的结果。这样心底才能“踏实”的接受这个知识点，因为它经过了实践的检验！

所有从事网络工作者，一定要不断的给自己创造参与实践的机会。如果在工作中能接触到现成的网络设备更好，这样学习起来更方便。要是达不到这种条件的话，可以参加一些培训班，它们多多少少都能提供一些操作实验。实在不行，就使用一些模拟器。它们所搭建起来的实验环境也很接近真实的网络环境。总之，一切网络知识，只有经过实践的检验，才能算它是正确的，也才能算自己真正掌握了它。

第6章

无线网络

记得有一位网络专家曾经说过，今后的数据连接介质就是光纤和无线，现在的双绞线、电话线和同轴电缆等会逐渐地被淘汰。此话深有道理，不赞成都不行。但此处我们只谈无线，光纤暂且不说。

无线网络确实是个好东西。可能这么说你还感觉不到，但是如果现在把所有的WIFI和移动数据网络都停掉，估计有一大片人都会疯掉！因为现在一大部分人的生活都是在移动网络上度过的，要是没网的话你让他怎么生活！

通常人们说的WIFI，就是指WLAN(Wireless Local Area Networks)无线局域网络，随着技术的不断发展，WIFI的传输速度也是突飞猛进，几十兆、几百兆的速度往上涨，但有的用户可能会很纳闷，WIFI的网速能达到几百兆，但我用手机上网怎么感觉这么慢啊！这往往是用户的一个错觉，上网慢有时并不是WIFI的网速慢，而是WIFI连接的上级网络速度慢导致的。

比如说你们家用的网是联通的网络，通常是联通公司的光纤会接入到你家里，在你家里会放置一个光纤猫，然后在光纤猫上会有一个网口，然后用一根短网线，一头连接光纤猫，另一头连接无线路由器的WAN口。可能有的家里不用光纤入户，也没有光纤猫，他们家里某一面的墙上就有网络信息点，信息点上有网口，也是拿一根网线，一端接墙上的信息点网口，另一端接无线路由器的WAN口。

还有重要的一步，就是要用家里的电脑连接到无线路由器上，进行路由器连接宽带用户名和密码，以及无线路由器无线网络的网络名和连接此网络的密码的设定，设定的方法一般在无线路由器的产品说明书中都会有详细说明，或者联通上门安装的服务人员会亲自给你进行配置的。

OK！这些都做完后，你就可以打开手机或笔记本，首先搜索你刚才在无线路由器上设定的无线网络名，单击连接，然后按照提示输入密码后，你就可以在互联网的世界里任性遨游了，想怎么玩就怎么玩！

WIFI的普及真是无处不在，现在你到一个地方的宾馆或者饭店等，可能首先要问的就是你这里有没有WIFI，密码多少？有一次我到一家饭店吃饭，我坐好后，就等着服务员把菜单拿过来我好点菜，但是我首先等来的不是菜单，而是

服务员递给我一个单子："先生，你好！这是我们饭店的WIFI名称和密码，祝你上网愉快！"，然后才是上菜单点菜，你看看，人家的服务多周到，体贴入微。

但是方便、易用的移动网络往往是一把双刃剑，它在把种种好处带给用户的同时，带给你的坏处也是大大的。

经常在网上会看到，用户的银行账户信息，邮箱密码等信息被无故盗用和泄露，这其中的一部分祸端就是无线网络引起的。WLAN网络在当初设计时，就有一个很大的安全缺陷，也就是在你的移动终端和无线路由器传输的数据都是明文传输，也就是不是通过加密的。如果你用手机给无线路由器发送的数据，包括有银行账户信息邮箱密码等，并且这些数据被黑客截获后，他们很快就能知道你的重要信息。

所以说在享受无线网络带来种种好处的同时，安全这根弦也是时时要绷紧。最重要和最基本的安全措施有两条，一是不要连接没有密码保护的WIFI，小便宜占不得，很有可能你连得就是非法的WIFI和黑客的无线路由器。二是自己的无线路由器要设置密码保护，而且密码的强度要高。总之，就是要采取一切办法把坏人、黑客拒之门外。

6.1　运维实例：小型路由器常见问题解析

目前，在很多单位都已经普遍使用小型路由器，常见的品牌有TP-Link、D-Link等。路由器具备的功能有路由、交换，有的还有无线功能。这种设备现在在家庭中使用也非常普遍，而且其无线功能使用的人越来越多。把路由器上的WAN口与ADSL Modem上的网口用网线连接起来，然后在路由器的LAN口上，就可接入多台终端设备，这样就有效扩展了用一根电话线访问互联网的终端数量。另外小型路由器的无线功能，可以让用户在信号辐射有效范围之内，随时随地方便地访问Internet，而不用再去连接繁琐的网线。

但是，随着小型路由器在网络中使用数量的增多，带来相关的故障也越来越多。下面就通过自己亲身经历的一则实例，让大家对小型路由器的功能和使用方法了解的更加透彻，若以后再碰到类似的故障，也不至于手忙脚乱。

1. 网络概况

网络结构图如图6-1所示，核心层交换机使用的是Cisco4506，接入层交换机使用的是Cisco3750。公司IP地址的部署，使用的是A类私有10网段的地址。DHCP服务器的IP地址为10.1.1.1。而TP-Link路由器上的用户，访问互联网时使用的IP地址是C类私有192网段地址，它是路由器自动分配的。Cisco4506和Cisco3750之间是Trunk连接。4506通过光纤连至互联网。

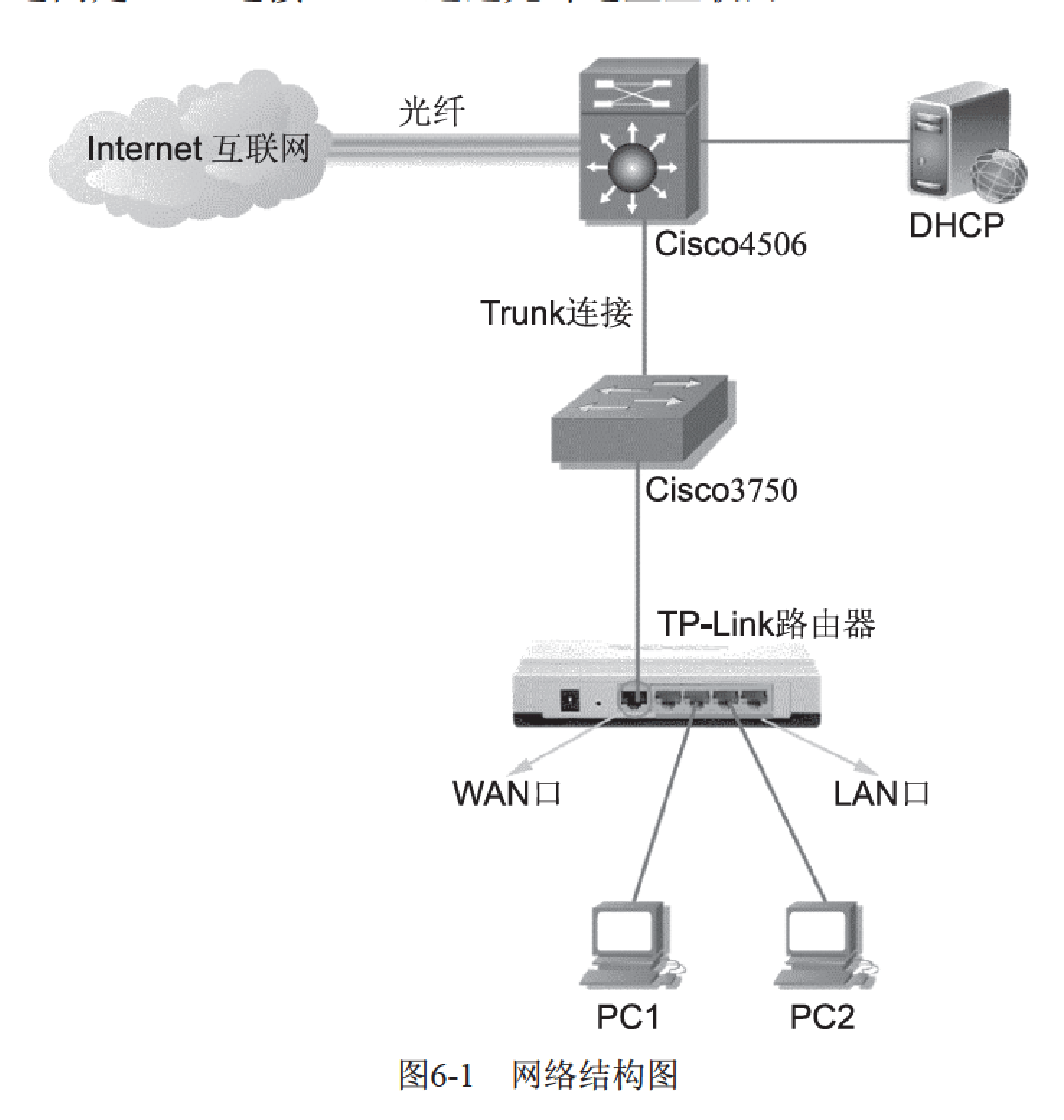


图6-1　网络结构图

2. 使用小型路由器的原因

使用的TP-Link路由器，有的有4个LAN口，有的有7个LAN口。它们在单位的普遍使用主要有两个原因。

一是，许多办公室的电脑在连至互联网时，办公室中电脑的数量，比房间中信息插座的数量要多很多，这样就不能保证把所有的电脑都接入到信息插座中。通过使用TP-Link路由器就能对办公室中的信息插座的数量进行有效的扩充。路由器的WAN口连至办公室中的一个信息插座上，然后在LAN口上就可接入用户的PC了，这样就把信息插座的数量从一个扩充到了4个或7个，也就能保证所有

的用户都连接到Internet上。

二是，有很多办公室，因为业务需求，需要组建自己的小型局域网。要求局域网外的用户不能访问到局域网内的数据，但要保证局域网内的用户都能访问到互联网。这种情况下，使用小型的TP-Link路由器也是很好的选择。路由器的WAN口连至网络中Cisco3750交换机上，然后路由器上所有的LAN口就构成了一个小的局域网。这时TP-Link上实际应用了NAT的PAT(Port Address Translation，端口地址转换)转换规则，在10网段中的一个IP地址及服务端口和192网段中的IP地址及服务端口之间建立了一个一一对应的关系。

3. 小型路由器在使用中带来的问题

小型路由器在公司使用数量的增多，相应地与之相关的网络故障也变得复杂起来。因为TP-Link路由器放在用户的办公室中，当用户不能正常访问互联网时，经常会私自改变路由器上的接线方式。如图6-2所示就是常见故障中的一种。

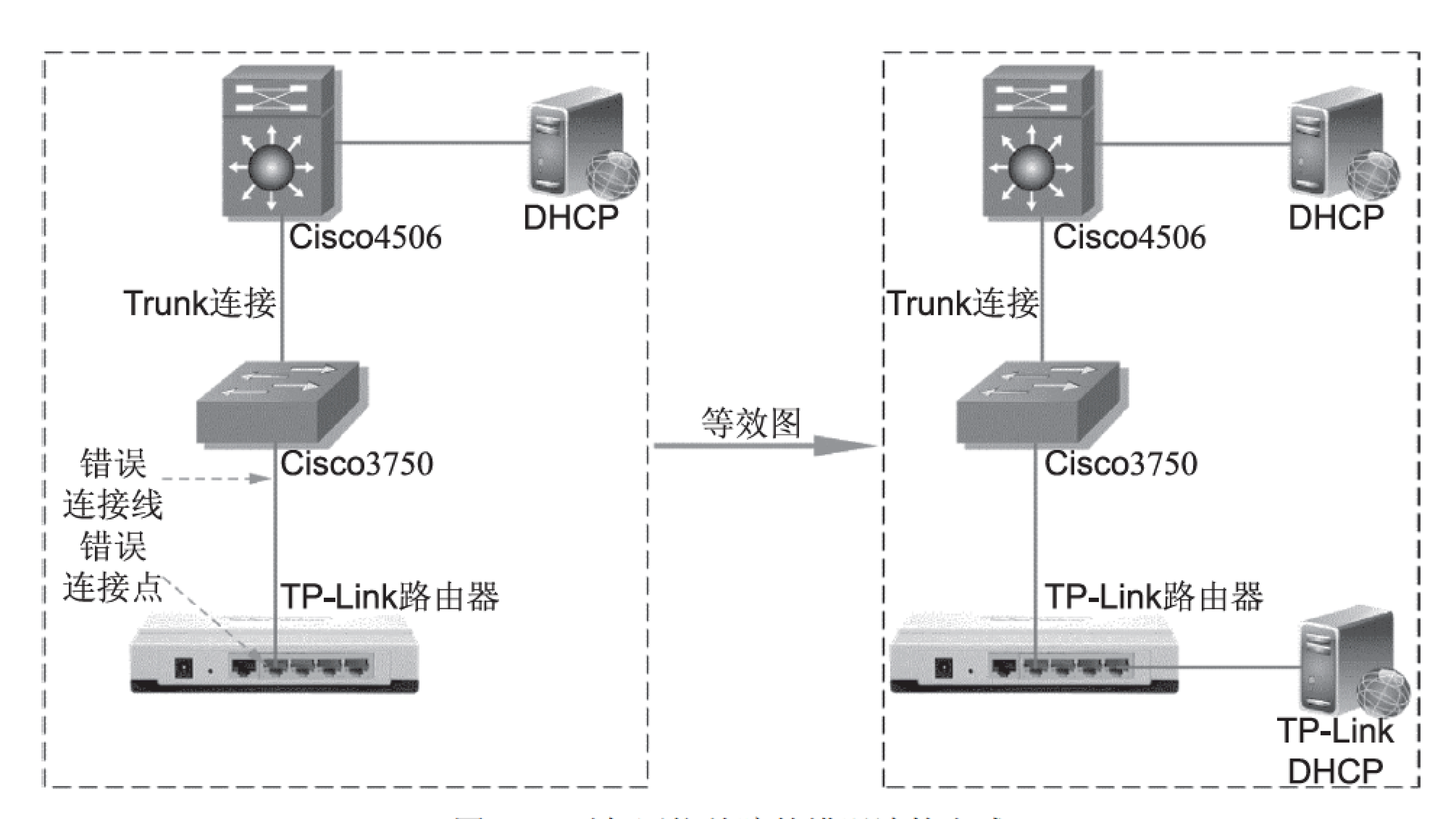


图6-2 引起网络故障的错误连接方式

图中的左边部分，是引起网络故障的错误连接，用户把连接到WAN口上的网线接到了LAN口上。这种错误的接入，严重的话可能会引起整个网络的瘫痪，因为TP-Link路由器在它的内部其实也内置了一台DHCP服务器，这样整个网络中就相当于有了两台DHCP服务器，如图6-2所示的右边部分，它其实和左边的网络是等效的。

单位大网中使用的是10网段地址，而TP-Link小的局域网中使用的是192网段的地址。用户在错误地连接TP-Link路由器后，网络中有很多用户电脑本来应该获取到的是10网段的地址，现在却获取到的是192网段的地址。而办公室局域网中的用户，本来应该获取到的是192网段的地址，而实际获取到的却是10网段的地址。错误的连接，导致单位网络客户端获取到错误的IP地址，进而导致大部分用户不能正常访问互联网。

4. 解决问题的两种方法

(1)网络中出现这种问题后，若要以最快的速度排除故障，其实只要把从Cisco3750接到小型路由器LAN口上的网线，再重新接到WAN口上就能使整个网络恢复正常。

(2)上面的方法，虽然排除故障的速度很快，但不能从根本上解决问题。因为用户若把网线再次错误接入，网络马上就会再次瘫痪。最彻底的办法就是把TP-Link路由器上的DHCP服务器功能关闭。

一般在连至TP-Link路由器LAN口上的电脑浏览器地址栏中，输入“http://192.168.0.1”，回车后就能进入TP-Link路由器的WEB管理界面，然后再进入DHCP服务器的设置界面，如图6-3所示。

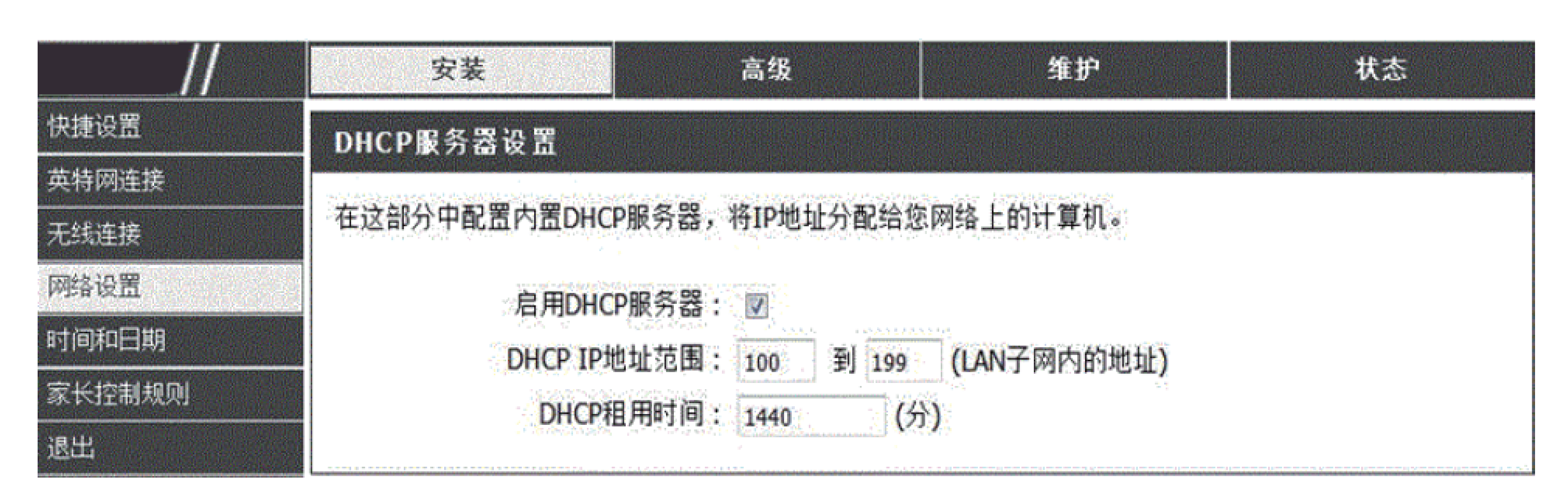


图6-3 关闭TP-Link路由器中DHCP服务器功能

把“DHCP服务器设置”中的“启用DHCP服务器”后面的勾去掉即可。然后把从Cisco3750上连至WAN口上的网线，连至LAN口上，也就是不再使用WAN口了。这样TP-Link路由器其实就变成了一台小型交换机。办公室中的用户若还要使用小型局域网的功能，只需在Cisco3750上配置相应的命令即可。这样就彻底避免了网络中有多台DHCP服务器时引起网络崩溃的故障。

5. 结束语

(1)小型路由器中一般都使用了两种重要技术：PAT和DHCP服务器功能。

①PAT(端口地址转换)。属于NAT中三大规则中的一种，另外两种是静态NAT(Static NAT)和动态NAT(Dynamic NAT)。PAT有时也称动态复用NAT，它改变了外出数据包的源端口，并进行端口转换，采用端口多路复用方式。内部网络的所有主机均可共享一个合法外部IP地址实现对Internet的访问，可以最大限度地节约IP地址资源。同时，也可以隐藏网络内部的所有主机，有效避免来自Internet的攻击。因此，目前网络中应用最多的就是PAT规则。

②DHCP服务器功能。当一台电脑第一次接入到，配置有DHCP服务器的网络中时，客户机上没有任何的IP数据设定，也就是没有IP地址、DNS和默认网关地址，这时它会向网络中发出一个 DHCP Discover数据包。因为客户端还不知道自己属于哪一个网络，所以数据包的源地址为0.0.0.0，而目的地址则为255.255.255.255 ，向网络进行广播。当客户端将第一个 DHCP Discover数据包送出去之后，在一秒之内若没有得到响应的话，就会进行第二次 DHCP Discover数据包的广播。若一直得不到响应的情况下，客户端一共会有四次 DHCP Discover数据包广播。

在DHCP服务器收到DHCP Discover发现报文后会做出响应，它从尚未出租的IP地址中挑选一个分配给DHCP客户机，并根据DHCP Discover数据包中原来携带的客户机MAC地址，向客户机发送一个包含出租的IP地址、DNS和默认网关地址的DHCP Offer提供报文。

如果网络中有多台DHCP服务器向客户机发来DHCP Offer提供IP地址，则客户机只接受第一个收到的DHCP Offer报文提供的IP地址。

从以上分析DHCP服务器的工作过程可以看出，当网络中有两个DHCP服务器运行的时候，客户机获取IP地址时，哪个DHCP服务器提供的速度快，客户机就采用那个DHCP服务器的提供的IP地址。所以，当把接入TP-Link的WAN口的网线接入LAN口后，网路中就包含了两个DHCP服务器。这样哪个DHCP服务器分发到客户端的IP地址速度快，客户端就采用了那个DHCP的IP地址，最终导致网络故障。

(2)网络的平稳正常运行，离不开科学的管理。用户出现不能访问网络的故

障，应当及时向网路管理部门上报，而不应私自处置。其次，应当禁止用户对放置在办公室中的小型路由器上的网线私自接入和拔出。如果单位的用户都能遵守网络管理规定，就不会引起网络瘫痪，其次在排除网络故障时，也就完全没有必要把小型路由器变成交换机使用了。

6.2 运维实例：SOHO路由器引起的IP地址冲突

SOHO路由器，目前在很多单位都已经普遍使用，好的品牌有Cisco、H3C，常用的品牌有TP-Link、D-Link等。SOHO路由器具备的功能有路由、交换，有的还有无线功能。这种设备现在在家庭中使用也很普遍，而且其无线功能使用的人越来越多。把路由器上的WAN口与ADSL Modem上的网口用网线连接起来，然后在路由器的LAN口上，就可接入多台终端设备，这样就有效扩展了用一根电话线访问互联网的终端数量。另外SOHO路由器的无线功能，可以让用户在信号辐射有效范围之内，随时随地方便的访问Internet，而不用再去连接繁琐的网线。

但是，随着SOHO路由器在网络中使用数量的增多，带来相关的故障也越来越多。下面就通过一则实例，让大家对SOHO路由器的功能和使用方法了解的更加透彻。若以后再碰到类似的故障，也不至于手忙脚乱。

1. 公司网络结构

网络结构图如图6-4所示。为了确保重要设备的稳定性和冗余性，核心层交换机使用两台Cisco4506，通过Trunk线连接。在接入层使用了多台Cisco3750交换机，图示为了简洁，只画出了两台。在核心交换机上连接有公司重要的服务器，如DHCP、E-MAIL服务器、WEB服务器等。公司IP地址的部署，使用的是B类私有172网段的地址。DHCP服务器的IP地址为172.16.1.1。Cisco4506和Cisco3750之间也是Trunk连接。4506通过光纤连接至互联网。

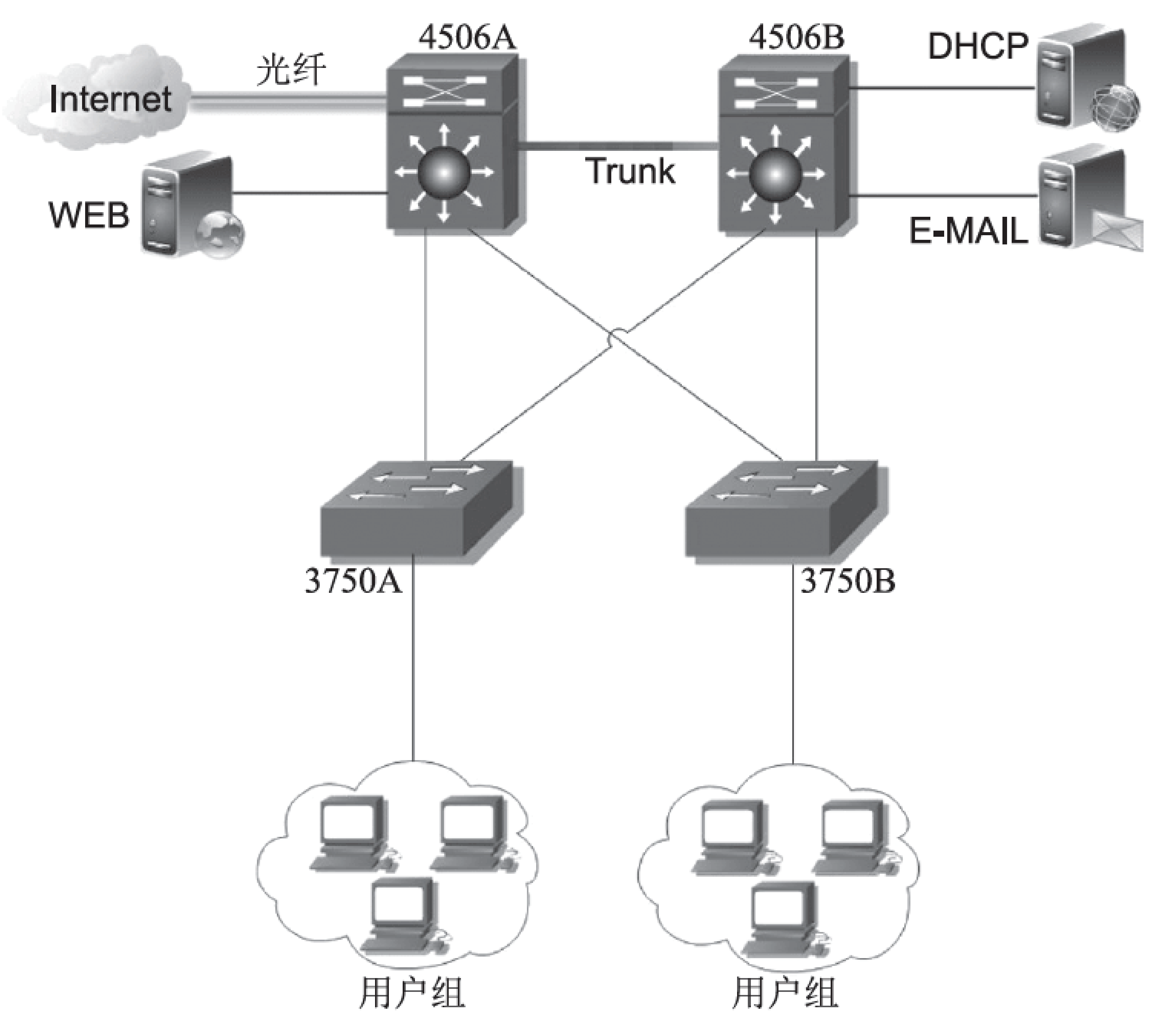


图6-4　网络结构图

2. 公司使用SOHO路由器的原因

公司使用的D-Link路由器，有的有4个LAN口，有的有7个LAN口。它们在单位的普遍使用主要有两个原因。

一是，许多办公室的电脑在连至互联网时，办公室中电脑的数量，比房间中信息插座的数量要多很多，这样就不能保证把所有的电脑都接入到信息插座中。通过使用D-Link路由器就能对办公室中的信息插座的数量进行有效的扩充。路由器的WAN口连至办公室中的一个信息插座上，然后在LAN口上就可接入用户的PC了，这样就把信息插座的数量从一个扩充到了4个或7个，也就能保证所有的用户都连接到Internet上。

二是，有很多办公室，因为业务需求，需要组建自己的小型局域网。要求局域网外的用户不能访问到局域网内的数据，但要保证局域网内的用户都能访问到互联网。这种情况下，使用小型的D-Link路由器也是很好的选择。路由器的WAN口连至网络中Cisco3750交换机上，然后路由器上所有的LAN口就构成了一个小的局域网。这时D-Link上实际应用了NAT的PAT(Port Address Translation，端口地址转换)转换规则。

3. 故障发生的过程

SOHO路由器在公司使用数量的增多，相应的与之相关的网络故障也变得复杂起来。因为单位新聘用了一名员工，要把他的PC接入到网络中，但接入时总提示“IP地址与网络上的其他系统有冲突”。后来，把电脑网卡上的网线拔掉再插上，让电脑重新从DHCP服务器获取IP地址，但故障依旧。接着又在电脑的“命令行”中用“ipconfig /release”命令释放网卡上的IP地址，然后再执行命令“ipconfig /renew”，让电脑再重新获取一次地址，但系统还是提示地址冲突。

接着，我们在“命令行”中执行“ipconfig /all”，发现电脑获取到的IP地址是172.16.11.34/24。既然提示说地址冲突，那么在网络中肯定还有一台设备在使用172.16.11.34这个地址。为了验证这种判断，先把新接入网络中的电脑关机，然后在网络中的其他电脑上，执行“ping 172.16.11.34”命令，结果和预期的一样，可以ping通。这就证明了，网络中还有一台设备正在使用172.16.11.34。接下来就是找出网络中的哪台设备在使用这个地址。

4. 排查故障的步骤

(1)按照当初网路的设计，客户端都是自动从DHCP服务器获取IP地址，也就是客户端使用的IP地址不是固定的。当从DHCP服务器获取的IP地址租用期满了之后，若再重新获取的话，IP地址就会有变化。但在网络的同一VLAN中使用172.16.11.34/24地址，可能有一百多台PC，总不能一台一台去查，这样效率太低。

(2)最终我们把寻找172.16.11.34/24的最好方法放在了Cisco4506和Cisco3750上，因为在三层交换机中都保存有ARP表，而在二层和三层交换机中都保存有主机MAC地址和交换机接口对应的二层CAM表。通过这两张表就很容易找到IP地址对应的设备。首先我们在Cisco4506上执行如下命令：

```
Cisco-4506#show arp | include 172.16.11.34
Protocol  Address   Age (min) Hardware Addr Type  Interface
Internet   172.16.11.34   8   00d1.8624.1a02   ARPA  VLAN11
```

上面命令显示的结果，只是4506中ARP表内容的一部分。通过它可以找到IP

地址172.16.11.34所对应的MAC地址00d1.8624.1a02。

(3)因为每一台电脑的MAC地址都是全球唯一的，所以我们再在Cisco3750上执行如下命令：

```
Cisco-3750#show mac-address-table dynamic | include 00d1.8624.1a02
Mac Address Table
-------------------------------------------
VLAN     Mac Address        Type          Ports
----    -------------      ----------    -----
11      00d1.8624.1a02     DYNAMIC       Gi1/0/13
```

上面命令的显示结果，也只是3750中CAM表内容的一部分。通过显示结果我们找到了IP地址是172.16.11.34的设备是通过3750的Gi1/0/13口连接到网络中的。然后我们再通过连接3750的Gi1/0/13口和机房中配线架的网络跳线，找到与Cisco3750 Gi1/0/13连接的配线架上端口对应的办公室房间号。结果，我们在那间办公室中找到了一台D-Link路由器。路由器在网络中的连接示意图如图6-5所示。

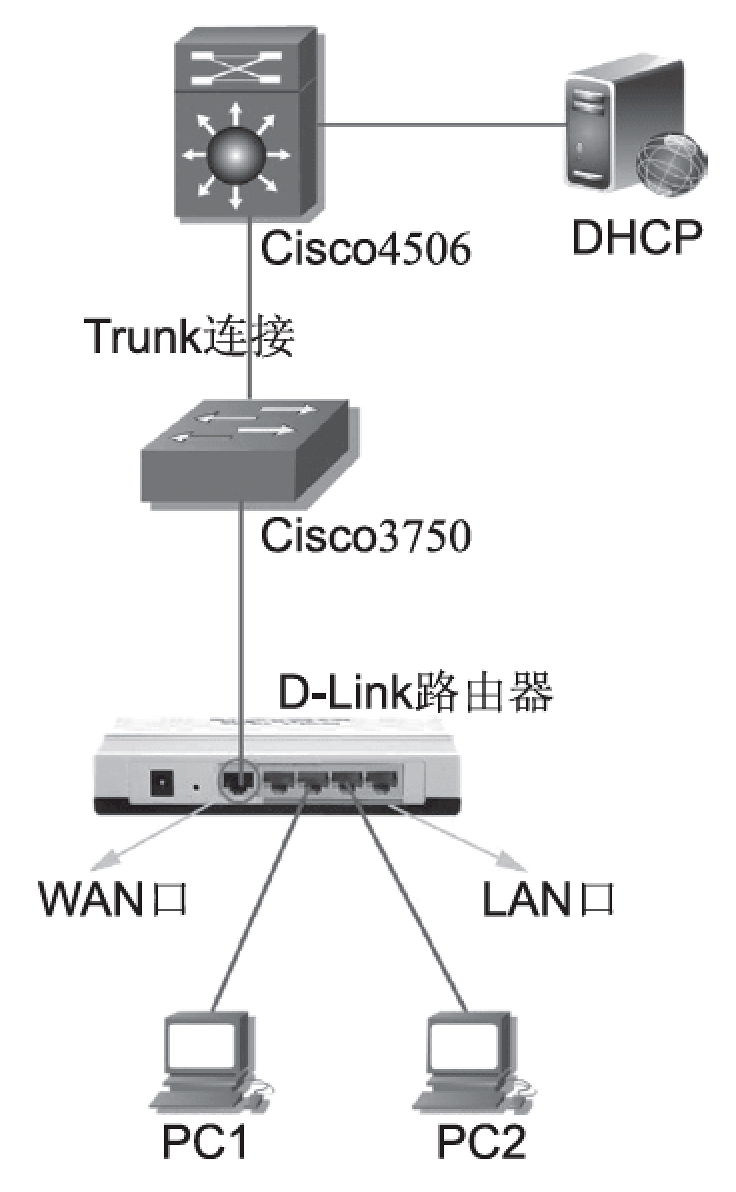


图6-5　引起地址冲突的路由器连接图

(4)接着在连接D-Link路由器的PC中的“命令行”中执行“ipconfig /all”命令，查找到D-Link路由器的网关地址是192.168.1.1，然后在PC的浏览器地址栏中输入192.168.1.1，进入D-Link的WEB配置管理界面。一般的SOHO路由器的管理配置都是以这种方式进入的。最后，在D-Link的WEB页面中找到了引起网络IP地址冲突的错误配置，如图6-6所示。



图6-6　D-Link路由器上的错误设置

(5)就是因为在此设备上也配置了静态的172.16.11.34/24地址，导致网络故障。要排除冲突故障，只要在WEB管理界面中的“因特网连接”→“因特网连接类型”中，选择“动态”，然后单击保存即可，如图6-7所示。

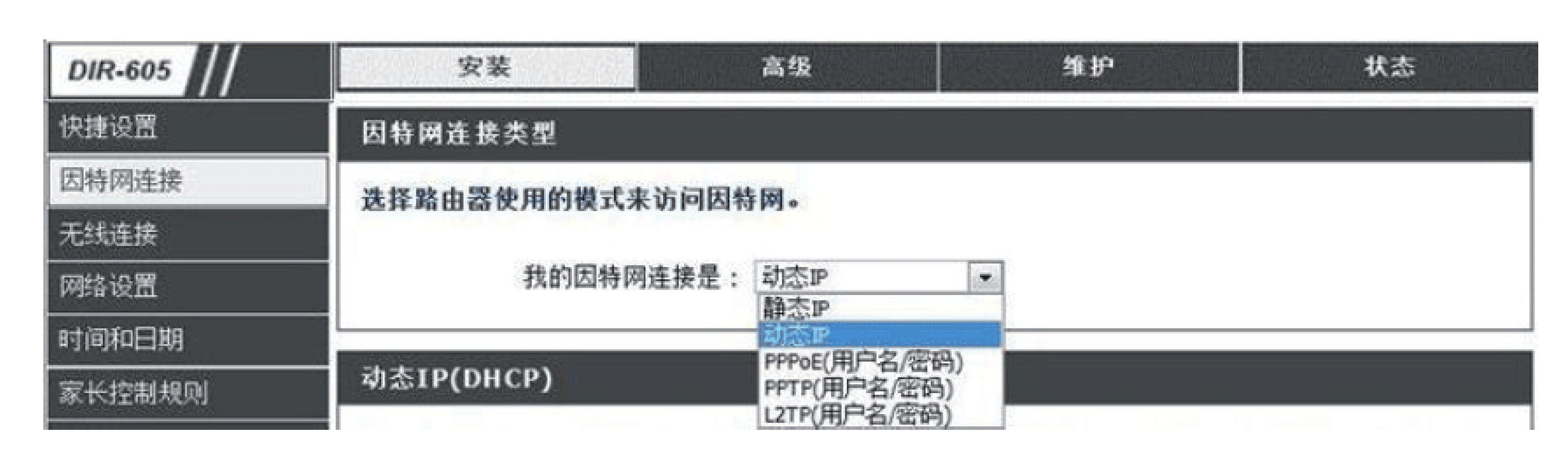


图6-7　排除IP地址冲突的正确设置

5. 总结

(1)SOHO路由器中一般都使用了两种重要技术：PAT和DHCP服务器功能。

①PAT(端口地址转换)。属于NAT中三大规则中的一种，另外两种是静态NAT(Static NAT)和动态NAT(Dynamic NAT)。PAT有时也称动态复用NAT，它改变了外出数据包的源端口，并进行端口转换，采用端口多路复用方式。内部网络的所有主机均可共享一个合法外部IP地址实现对Internet的访问，可以最大限度地

节约IP地址资源。同时，也可以隐藏网络内部的所有主机，有效避免来自Internet的攻击。因此，目前网络中应用最多的就是PAT规则。

②DHCP服务器功能。当一台电脑第一次接入到配置有DHCP服务器的网络中时，客户机上没有任何的IP数据设定，也就是没有IP地址、DNS和默认网关地址，这时它会向网络中发出一个 DHCP Discover数据包。因为客户端还不知道自己属于哪一个网络，所以数据包的源地址为0.0.0.0，而目的地址则为255.255.255.255，向网络进行广播。当客户端将第一个 DHCP Discover数据包送出去之后，在一秒之内若没有得到响应的话，就会进行第二次 DHCP Discover数据包的广播。若一直得不到响应的情况下，客户端一共会有四次 DHCP Discover数据包广播。

在DHCP服务器收到DHCP Discover发现报文后会做出响应，它从尚未出租的IP地址中挑选一个分配给DHCP客户机，并根据DHCP Discover数据包中原来携带的客户机MAC地址，向客户机发送一个包含出租的IP地址、DNS和默认网关地址的DHCP Offer提供报文。

(2)对故障的深入分析。通过上面对DHCP工作原理的分析，发现当网络中SOHO路由器上也配置了静态的172.16.11.34地址后，若再有PC接入到网络中，DHCP给PC分配IP地址时，因为它并不知道172.16.11.34已在网络中配置，所以它还是按照IP地址分配的顺序，前面172.16.11.1～33的地址已经分配，自然就把172.16.11.34分配给了新加入网络中的PC，从而造成了冲突故障。

(3)CAM表和ARP表。在二层和三层交换机上都会维护一张用于二层交换的地址表，即CAM表。该表是MAC地址与交换机出接口的对应关系。这样当收到一个以太网数据帧时，交换机判断如果该数据帧不是发送给自己的，则根据数据帧的目的MAC地址查询CAM表，如果能在CAM表中找到与该MAC地址对应的转发项，则根据查询的结果，通常是一个出接口列表，在相应的接口上把数据帧转发出去。如果不能找到，则向所有端口广播该数据帧。

在网络中的三层设备上都会维护一张ARP表，用于查找连接到三层设备的客户端或服务器的IP地址和其MAC地址。也就说只要知道MAC地址和IP地址其中的一个就可以知道另外一个。通常在网络中利用这两张表就可以迅速地确定一个设备的具体位置。

第7章 应用系统

信息化在一个单位的建设实施，最直观的反映就是一个个的应用系统。OA(Office Automation)办公自动化系统、档案系统、人事系统和财务系统，这些系统都是基本的，一般的单位都有。每个单位有每个单位侧重的专业，相应的在信息化建设方面，就要部署对应的应用系统，像在传媒出版集团，就要有编排应用系统、出版发行系统等，在军事工业集团就要有产品测试系统、军事演练系统等。

随着信息化建设规模的不断扩大和计算机应用的不断推广，各单位的应用系统建设也是与日俱增，就比如现在的移动终端使用非常广泛，最主要的原因是移动终端上的应用给用户带来了实实在在的好处。

现在流行的移动办公，就是把原来在电脑台式机上办公的部分内容，迁移到移动终端上，实现用户在手机上也可以登录到单位的办公系统、财务系统等。这些功能的实现，就少不了进行后台系统的开发，而且要实现好的用户体验，还要有针对性的开发，比如对Android和苹果IOS两类不同移动终端系统的开发。

确定用户好的体验是和后台开发和运维人员的辛苦努力是分不开的，用户的体验越好，他们就越辛苦。以前的应用系统，只应用在台式机或笔记本上，现在多出了在移动端的应用系统，运维人员的工作量也要随之增加。

应用系统的上层是具体的用户，应用系统的下层就是网络支撑平台——网络系统。所以，应用系统在一个单位的信息化部门中是起着承上启下的作用的。

没有一个好的网络基础平台，再好的应用系统也发挥不出它应有的作用，也不会有好的用户体验。一个好的网络基础支撑平台，若没有高效的应用系统在它上面运行，也体现不出它应有的价值。所有的网络支撑平台和应用系统平台二者之间是相辅相成，缺一不可的。

这在一个单位的信息化管理部门的运作上也能够反映出来，通常是用户反映某个应用系统无法使用时，系统运维人员和网络运维人员就要密切合作，一点点排查可能引起问题的故障点，直到最终找到故障真正原因。

作为网络运维人员，在专业水准上不可能达到系统运维人员的水平，但是要

掌握应用系统的基本知识也是必不可少的，本章节是叙述一些应用系统的基本知识，主要包括Windows系统、Linux系统和应用系统的运维管理软件等。

7.1 运维实例：搭建Linux学习环境的5种方法

目前，Windows在个人版电脑操作系统中占据着绝对的优势，但是在服务器操作系统方面，却不再是Windows一家独大，这多少能让人感到不少欣慰，因为Unix、Linux是绝对可以和微软相抗衡的。甚至，在许多单位Unix和Linux的部署已远远超过了Windows系统，尤其是Linux的应用更多。

Linux系统不像Windows系统，所有的操作都能在“窗口”中完成，虽然Linux也有图像化的操作界面，但其功能远远不能和Windows相提并论。它绝大部分的功能都要通过“终端”命令行的模式去完成。学习Linux系统最好的方法就是搭建真实的Linux学习环境。现在个人电脑都已经非常普及，在电脑上安装一个Linux系统，不就很快搭建起一个Linux的学习环境了吗？但它未必是最好的方法。下面就把搭建Linux学习环境的5种方法介绍如下，看看哪一个是最适合你的方法。

1. 在Windows服务器上安装VMware，并在VMware中安装Linux系统，然后通过远程登录到Windows服务器上的VMware，学习Linux

搭建这种环境的过程是这样的，因为单位有一台联想的服务器，安装的操作系统为Windows 2003，对外提供WEB服务，IP地址为21.89.54.213。但服务器上的WEB应用占据服务器上的硬件资源却非常少，并且它对可靠性的要求不是很严格，不过还是每天24小时开着机。服务器上就跑一个很简单的WEB应用，这对服务器的硬件资源其实是一种很严重的浪费，它上面的CPU、内存根本没有使用多少，所以就想到何不在服务器上安装一个Linux系统，把服务器当成个学习的工具，这样既充分利用了服务器的硬件资源，同时它也具备了真实的Linux系统学习环境。

但服务器上已经安装了Windows 2003，而且要保证它7×24小时连续运行，所以再在服务器上安装个Linux系统成为双系统不太现实。所以后来就想到在

Windows 2003中安装VMware软件，然后再在VMware中安装Linux系统，这样在不影响服务器对外提供WEB服务的同时，也能在服务器上学习Linux系统，而且这样也提高了服务器的硬件资源利用率。

这种环境的搭建，比在个人电脑上安装Linux系统要好很多，因为个人电脑毕竟是个人版，各方面的硬件配置不能和服务器相比，而且Linux系统本身作为服务器操作系统使用的占多数，所以在服务器上搭建Linux学习环境是最好的选择。

这种环境还有一个好处，就是只要在有网络和Windows系统的地方，就能很方便地登录到服务器上，进入到Linux系统的学习环境中，熟悉各种命令的使用。首先，利用Windows系统的“远程桌面连接”功能，如图7-1所示，在对话框中输入单位联想服务器的IP地址21.89.54.213，单击“连接”，根据提示输入用户名和密码，就能远程登录到联想服务器上的Windows 2003操作系统上，然后再在Windows系统中运行VMware，然后在VMware中再打开Linux系统，本例中使用的Linux系统是Red Hat Enterprise Linux 5，然后就可以正常使用Linux系统了，如图7-2所示是通过远程桌面连接，登录到远程Windows 2003服务器VMware中的Linux操作系统上。

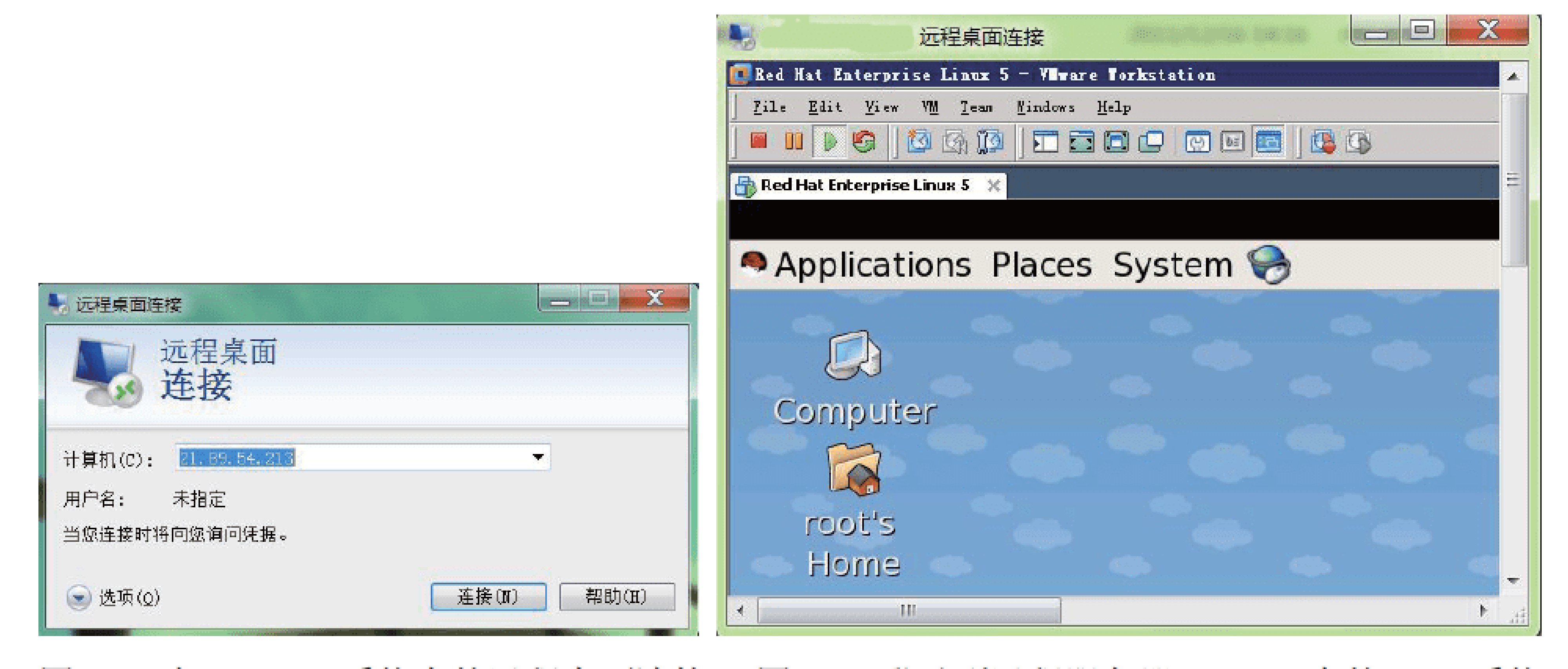


图7-1　在Windows系统中的远程桌面连接　图7-2　登录到远程服务器VMware中的Linux系统

上面的操作，还有一点需要注意的就是，首先要在联想服务器上的Windows 2003中开启“允许远程桌面的计算机连接到本系统”，也就是开启允许远程桌面连接的功能。当你在远程想关闭这种Linux的学习环境，只要直接关闭Windows 2003中的VMware即可。但是，在关闭时，VMware会显示一个关闭的对话框，如

图7-3所示，有三个选项“Suspend”“Power Off”和“Run in Background”，选择第一个就行，它意思就是把Linux系统“挂起”，但其实并没有关闭系统。

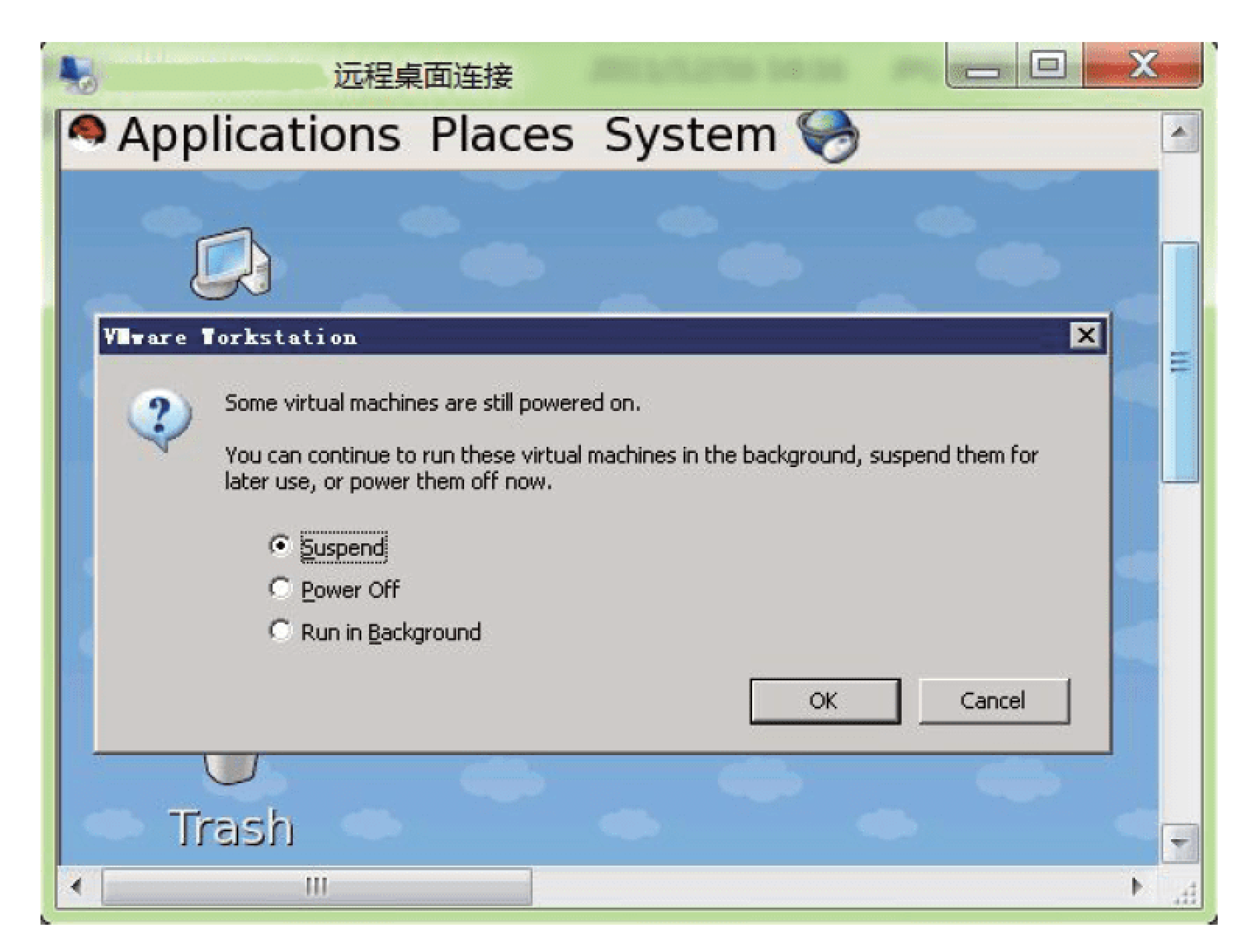


图7-3　关闭VMware Workstation的三个选项

当下次再远程登录到Windows 2003服务器上，想学习Linux命令时，直接打开VMware即可，但这时VMware会有一个选择打开Linux系统的方式，如图7-4所示。这时应选择“Commands”对话框中的“Resume this virtual machine”选项。这样就会马上进入Linux系统中，根本没有启动Linux系统一连串的过程。就和Windows系统从“待机”或“休眠”状态进入到系统中的速度一样快。若在上面关闭VMware时，选择的是“Run in Background”的选项，则下次打开VMware时，比选择“Suspend”速度更快，立刻就会进入了Linux系统。但选择“Run in Background”关闭VMware Workstation后，它仍然会占用非常多的服务器硬件资源，所以不推荐使用这种方式关闭。除非是关闭后，又很快想回到操作系统的界面。

而且这种学习模式，在VMware中的Linux系统中进行任何的操作和测试，都不会影响到Windows 2003系统上的WEB应用，这样就给学习Linux的用户带来了极大的自由和方便，不必有任何的顾忌。

可能有的人觉得在远程直接登录到装有Linux系统的服务器上不就行了吗？但这其实并不是很方便，因为目前的个人用户大部分使用的都是Windows系统，

要在Windows系统上登录到远程的Linux系统上，不仅要在Windows系统上安装专门的软件，而且还要在远端的Linux服务器上进行多个步骤的设置才能支持这个功能。这种模式的搭建将在下面进行详细的介绍。而且若登录到的Linux服务器上，有一些应用系统正在运行的话，这样在学习Linux命令的同时，总是蹑手蹑脚不敢操作，生怕影响到了服务器上的应用。

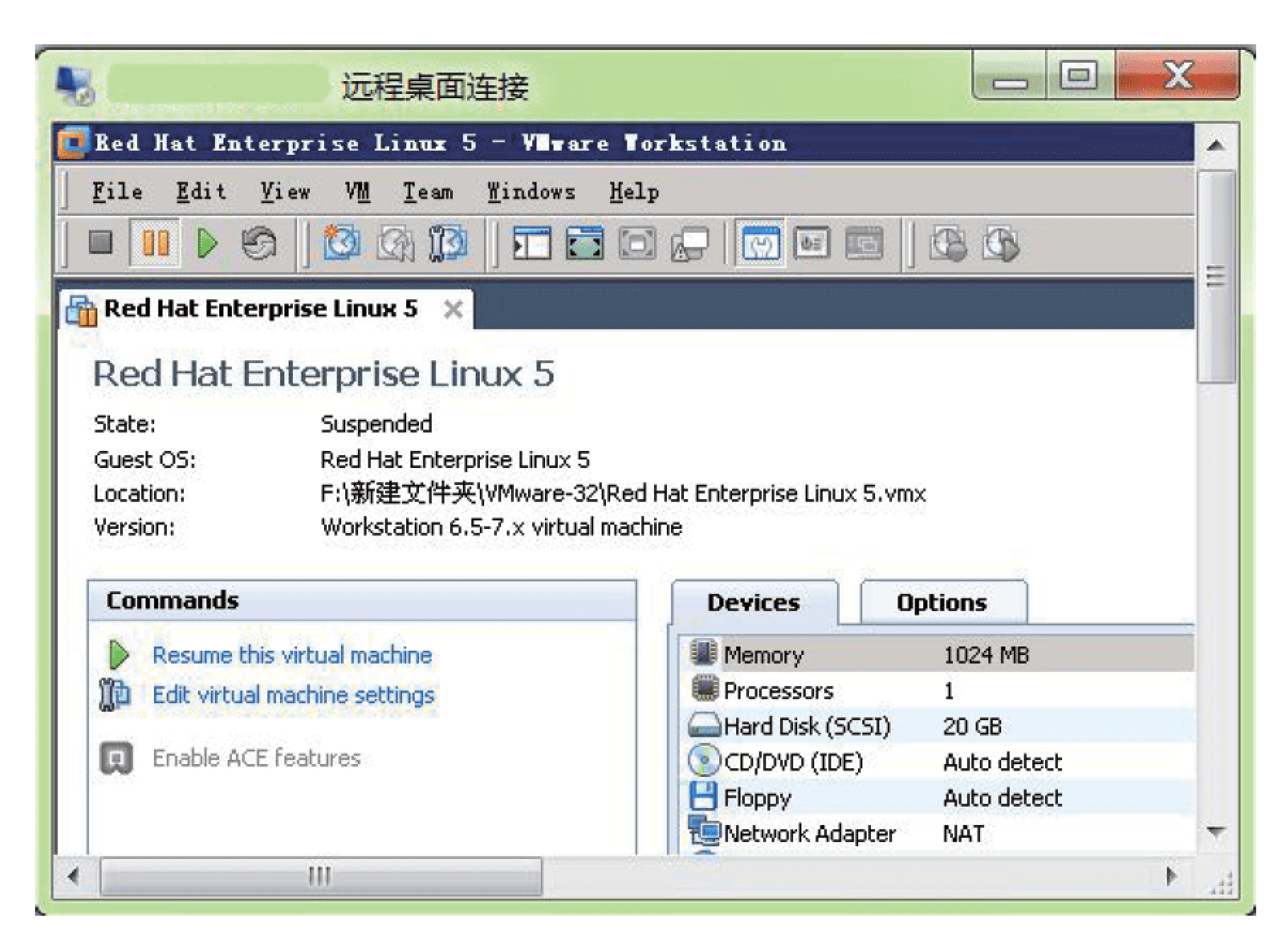


图7-4　快速进入到Linux系统的操作图示

若是在公司找一个服务器搭建这种学习环境困难的话，就是用一个性能不错的台式机代替服务器也是可以的，只要能保证它24小时运转就行。按照上面的步骤在台式机上先安装Windows系统，再装VMware和Linux。然后把台式机挂到外网上，这样就是你下班回家后想再学习Linux，可以通过家里的ADSL远程登录到单位的台式机上，然后就能很快地进入到Linux的学习环境中，进行各种命令的学习了。这也就是说，只要在有网络和电脑的地方，总能让你马上登录到Linux系统中。这样就给大家提供了很大的便利，节省了时间提高了效率。

2. 在Windows系统下安装Linux系统，形成双系统

这种双系统的模式可能有很多人都安装过，但它使用起来并不是很方便。因为开机后，选择进入了其中一个操作系统的话，若再想进入另外一个系统，就得重新启动电脑，不方便，也浪费时间。不过它也是一种建立学习Linux系统环境

的方法。

Windows和Linux双系统的安装方法，在网上有很多，这里就不再啰嗦了，大家也可以参考“http://529462.blog.51cto.com/519462/622244”来进行安装。它是介绍在目前普遍使用的Win 7下安装Red Hat 6的详细步骤。需要注意的是：

(1)安装过程可以不使用安装光盘，直接使用网上下载的Linux ISO就可以。

(2)EasyBCD软件版本的选择最好和介绍的使用一样，因为不同版本在操作的界面和操作的步骤上会有很大不同，为了达到最大化的“傻瓜”式操作，还是选择EasyBCD 2.0 BEAT版本比较好，这样在安装的过程中也节省了你的时间。

(3)在使用EasyBCD软件的过程中，要复制粘贴一段代码，如下所示：

```
title install linux
root (hd0,1)
kernel (hd0,1)/isolinux/vmlinuz initrd
(hd0,1)/isolinux/initrd.img
```

代码“(hd0,1)”中的数字的选择其实是很灵活的，不一定非要是括号中的数字，主要是根据自己电脑的实际配置情况选择合适的数字就行，可以多试几次，肯定能选到正确的。

3. 在Windows系统中安装VMware，然后再在VMware中安装Linux系统

这种Linux学习环境的搭建其实在“1”中已经应用到了，安装过程和第“2”种在Windows下安装Linux系统的过程大同小异，只不过一个是在电脑上直接安装，一个是在VMware中安装。

需要注意的是，如果是在Win 7系统下的VMWare中安装Linux的话，一是用ISO映像不是很好安装，最好直接用光盘装肯定没问题；二是若安装的是Linux 64位操作系统的话，要在电脑的BIOS中，开启支持64位功能和虚拟技术的参数，如“Intel(R)Virtualization Technology”“Enable VT-d”两个参数。

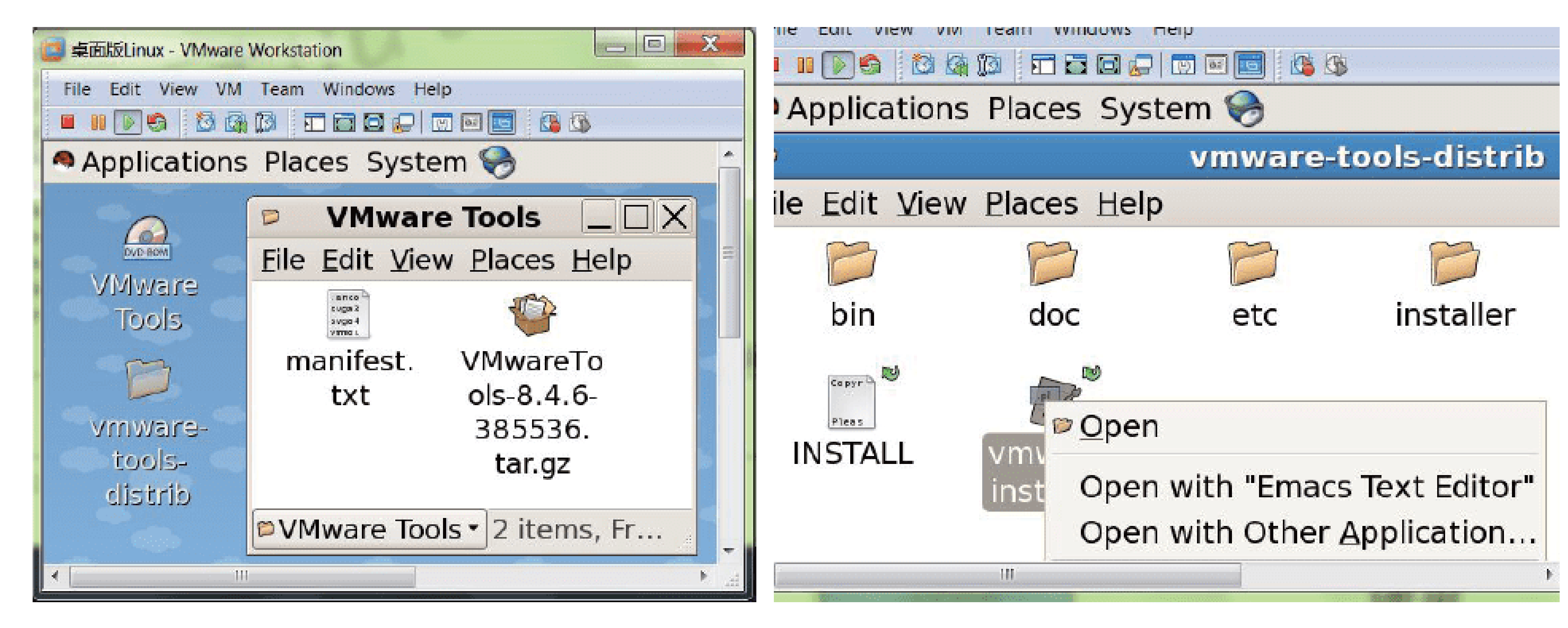


图7-6　解压光驱中的压缩文件　　　　图7-7　执行“vmware-install.pl”文件图示

(3)安装完成，重新启动系统后，会发现Linux系统的显示屏要比原来的大了很多。鼠标指针也可以在Linux和Windows系统之间平滑过渡，不需再使用Ctrl+Alt组合键了。

(4)可以在Windows和Linux系统之间共享文件夹。在Windows系统中设置共享文件夹的位置，是在VMware Workstation上配置的，在菜单栏选择“VM”→“Settings”→“Options”→“Shared Folders”，然后在右边单击Add按键，选择共享文件夹在Windows系统中的目录位置，如图7-8所示。然后，在Linux系统中进入到“/mnt/hgfs/Sharing”目录下，就可以看到和Windows系统中共享文件夹中相同的内容，也可以在Linux下将文件拷贝到此文件夹传递到Windows下。

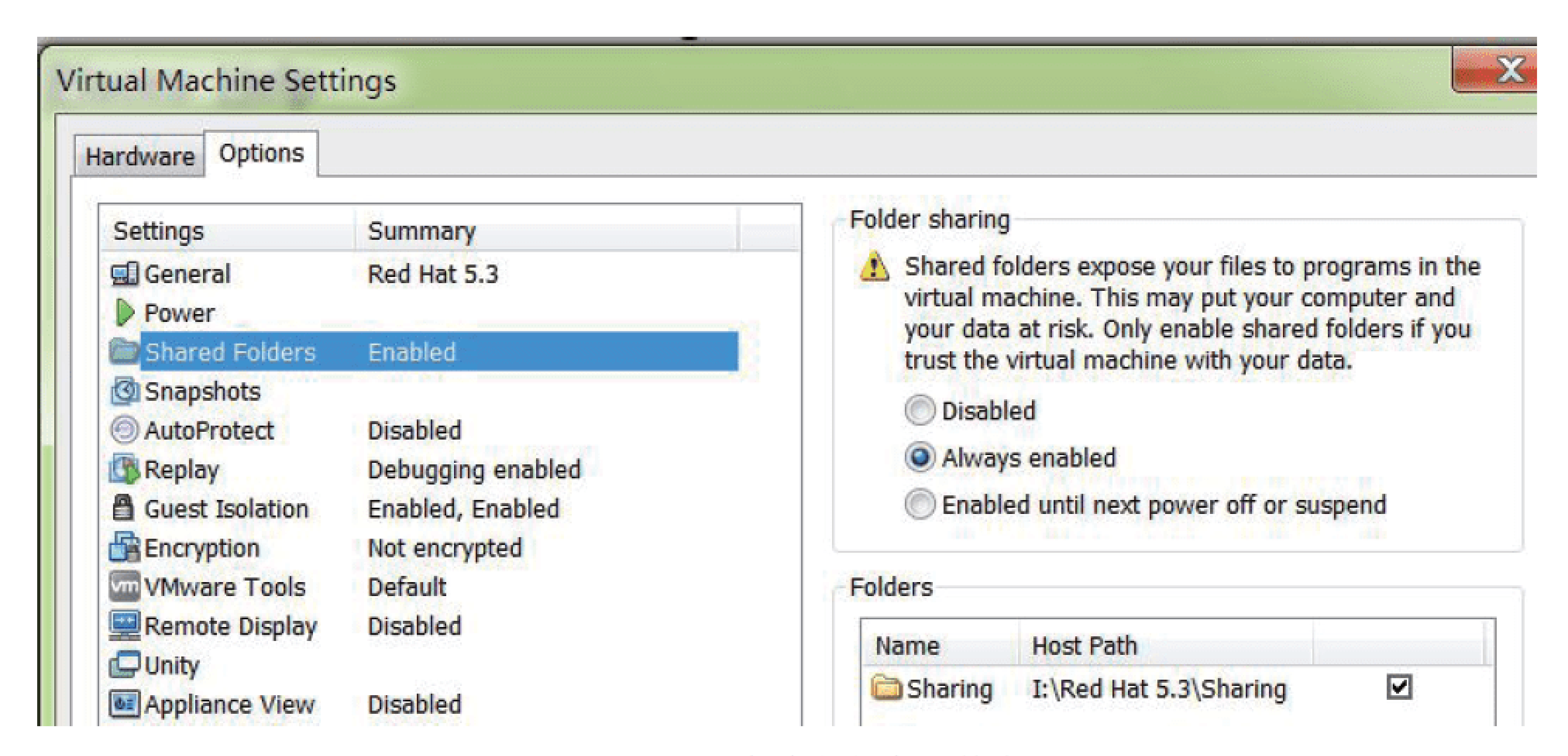


图7-8　Windows中建立共享文件夹图示

(5)默认情况下，虚拟Linux系统的网络模式是NAT模式，这种情况下，在VM中虚拟的Linux系统也可以通过Windows系统的主机访问到互联网，但前提是

```
[root@localhost .vnc]# rpm -ivh vnc-4.1.2-14.el5.x86_64.rpm
warning: vnc-4.1.2-14.el5.x86_64.rpm: Header V3 DSA signature: NOKEY, key ID 37017186
Preparing... ########################################### [100%]
 package vnc-4.1.2-14.el5.x86_64 is already installed
```

(3)编辑“.vnc目录”下的“xstartup文件”。可以使用VI编辑器进行编辑，命令为“[root@localhost .vnc]#vi xstartup”，打开“xstartup”文件后在键盘上单击“A”字母键，使VI编辑器进入编辑状态。然后屏蔽掉最后一行，即在最后一行的前面加上符号“#”，变成“#twm &”，然后再在最下面加上“gnome-session &”。完成后，单击“Esc”键，再单击“：”键，然后输入“wq”回车，即保存退出。加上“gnome-session &”是为了能够在Windows系统上显示Linux的桌面，否则只能看到一个“终端”的命令行窗口。

(4)设置登录用户。如果上面的安装成功，在目录/etc/sysconfig/下会有一个vncservers文件。用VI编辑器编辑vncservers文件，在最后加上VNCSERVERS=“1:root”，保存后退出。

(5)设置VNC远程登录密码。运行命令“[root@localhost ～]# vncpasswd”，然后按提示设置好远程登录的密码。然后执行命令“[root@localhost ～]#vncserver”，会有如下显示：

```
New ‘localhost.localdomain:1 (root)’ desktop is localhost.localdomain:1
Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/localhost.localdomain:1.log
```

这里需要注意的是，上面的输出“localhost.localdomain:1 (root)”，说明在用浏览器远程登录Linux系统时，在浏览器地址栏中要输入的地址为“Linux服务

若在VNC Viewer的“Server”地址栏中输入的IP地址后面所接的端口号，不是“localhost.localdomain:1 (root)”中的“1”，而是写成了其他的数字，那可能只能进入Linux系统的终端命令行模式，而进入不到图形化的桌面模式。

5. 用SSH方式登录到远程服务器的Linux系统中

其实和SSH登录方式非常相像的还有Telnet登录，但因为Telnet登录的用户名和密码以及在配置管理当中所使用的Linux命令都是以明文的方式传送的，没有任何的安全措施，所以目前它基本上已经被SSH的登录方式所取代。SSH服务在Linux下的设置非常简单。下面就简要地介绍一下SSH服务的设置与登录的步骤：

(1)SSH服务的安装状态。此服务默认是安装的，但也可以通过以下命令来查询在Linux系统中是否安装了SSH服务。

```
[root@localhost ~]# rpm -qa | grep ssh
openssh-clients-4.3p2-29.el5
openssh-4.3p2-29.el5
openssh-askpass-4.3p2-29.el5
openssh-server-4.3p2-29.el5
```

若出现以上的显示结果，则表示此Linux系统已经安装了SSH服务。输出内容的第一行显示的是SSH的客户端软件包；第二行显示的是SSH的核心文件；第三行表示SSH支持对话框的显示，是一个基于X系统的密码诊断工具；第四行是SSH的服务器软件包。

(2)SSH服务的运行状态。此服务默认也是自动运行的，但也可以通过以下命令来查询SSH服务的运行状态。

```
[root@localhost ~]#service sshd status
openssh-daemon (pid  5340)is running...
```

若出现以上的显示结果，则表示此Linux系统的SSH服务已经运行。其中，“sshd”是SSH服务的守护进程名称。若SSH服务没有启动的话，则运行命令[root@localhost ~]#service sshd restart即可。

(3)用SSH进行远程登录的设置。若是在Windows系统中没有自带的SSH客户端，可以在网上下载支持SSH远程登录的图形化工具软件，常用的有SecureCRT、Putty等。如图7-12所示，是用SecureCRT进行远程SSH登录的设置。在“Hostname”中输入SSH服务器的IP地址，“Port”中输入22，“Username”中输入用户名。然后根据提示，输入密码，就可以连接到远程的SSH服务器。若是在Linux系统中进行远程的SSH登录，就可以在Linux的终端窗口的命令提示符下，直接使用命令#ssh 192.168.1.2进行远程登录即可。

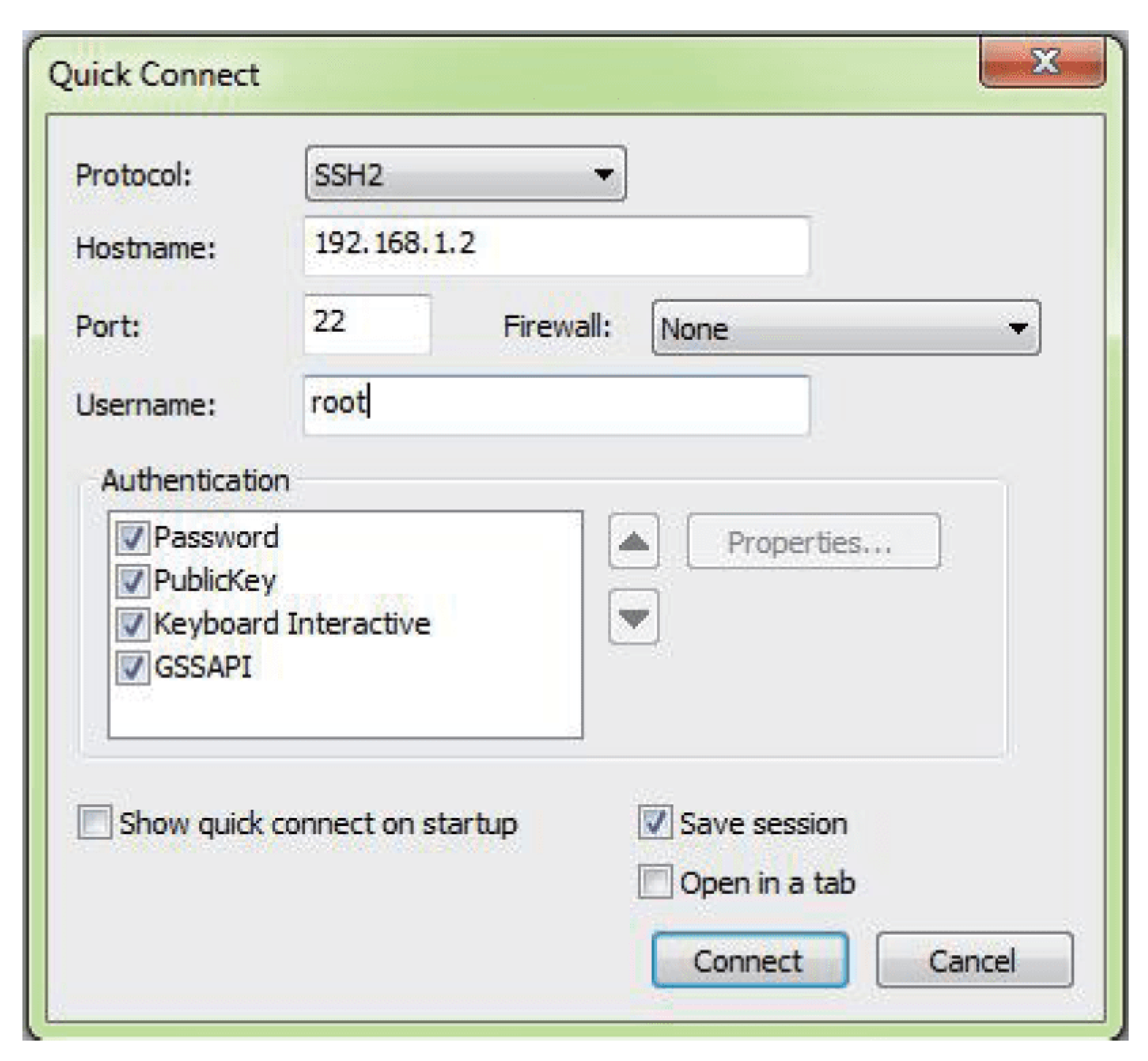


图7-12　用SecureCRT以SSH方式登录的参数设置

(4)SSH的配置文件。SSH有两个主要的配置文件，一个为客户端的配置文件ssh_config，另一个为服务器端的配置文件sshd_config。这两个配置文件都位于目录/etc/ssh下。用VI编辑器就可以对这两个配置文件进行详细的配置和修改，以便用户在使用SSH时能满足一些特殊的要求。

较快捷的方法是可以结合使用EasyBCD软件进行Red Hat系统的安装。安装过程需要注意两点：

(1)安装过程可以不使用安装光盘，直接使用Linux ISO镜像文件就可以，这种方式比较方便快捷。

(2)在使用EasyBCD软件，安装Red Hat的过程中，其中要给一个记事本文件中，复制粘贴一段代码，如下所示：

```
title install linux
root (hd0,1)
kernel (hd0,1)/isolinux/vmlinuz initrd
 (hd0,1)/isolinux/initrd.img
```

其中，代码“(hd0,1)”数字的选择其实是很灵活的，不一定非要是括号中的数字，主要是根据自己电脑的实际配置情况选择合适的数字就行。可以多试几次，肯定能选到正确的。

2. 在电脑的Win 7系统中删除RedHat系统

在Win 7操作系统桌面的“计算机”图标上单击右键，选择“管理”进入到“计算机管理”的界面中，选择“存储”中的“磁盘管理”。然后在右边的显示栏中就可以直接看到安装了Red Hat操作系统的盘符，在盘符上单击右键，选择“格式化(F)...”直接对安装了Red Hat操作系统的分区，进行格式化。格式化完成后，也就把电脑上的Red Hat操作系统删除了。

但是在Win 7操作系统中，格式化掉Red Hat系统所在的分区后。每次重新启动电脑后，首先进入的还是GNU GRUB的启动管理界面，然后选择是进入Red Hat还是进入Win 7系统，如果不进行选择的话，它默认还是进入了Red Hat系统中，如图7-13所示。所以，电脑在默认的情况下，开机后还是不能自动进入到Win 7系统中。这是因为，在电脑上安装了Win 7操作系统后，再安装Red Hat系统，会修改电脑上的主引导记录(Master Boot Record，MBR)，它又叫做主引导扇

区，是计算机开机后访问硬盘时所必须要读取的首个扇区。

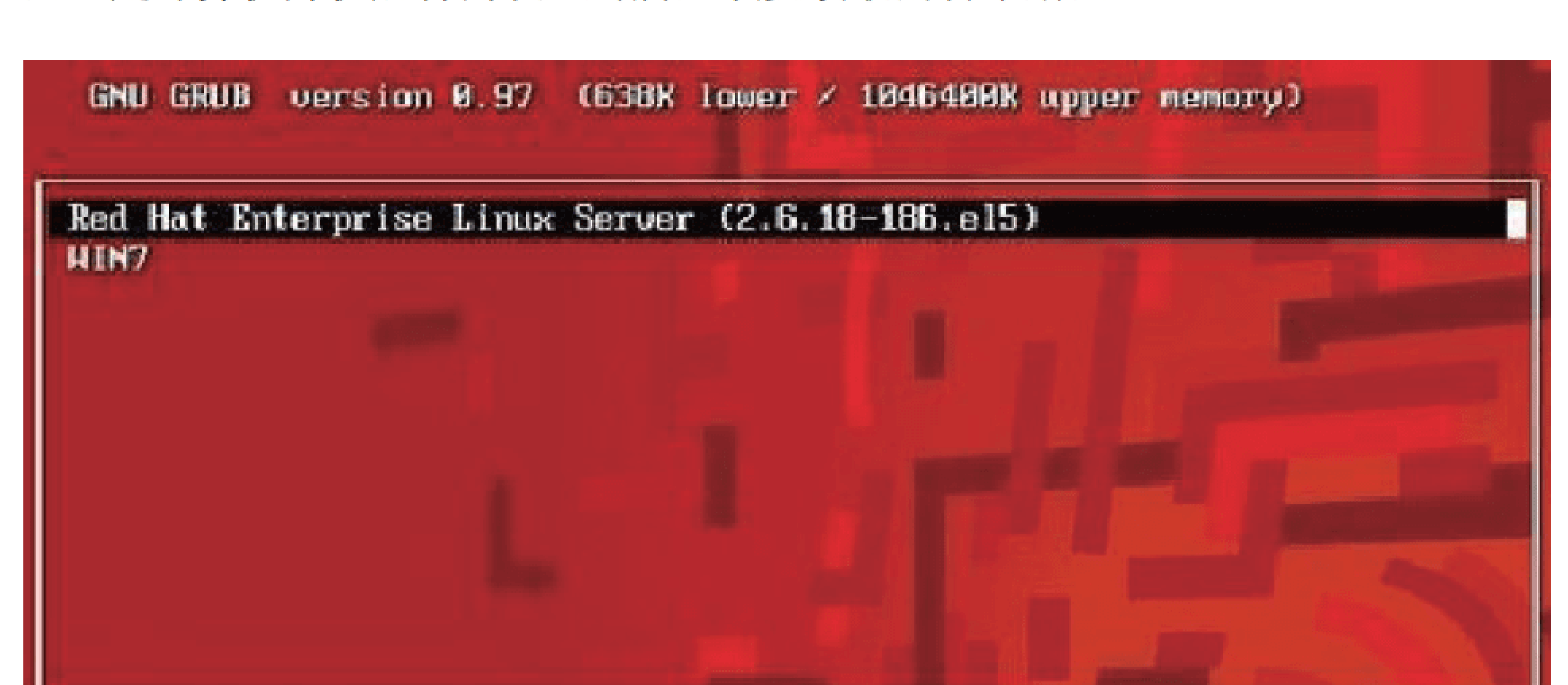


图7-13　GRUB中选择进入操作系统的界面

MBR记录着硬盘本身的相关信息以及硬盘各个分区的大小及位置信息，是数据信息的重要入口。如果它受到破坏，硬盘上的基本数据结构信息将会丢失，需要用繁琐的方式试探性地重建数据结构信息后才可能重新访问原先的数据。主引导扇区内的信息是通过FDISK写入的，它是低级格式化的产物，和操作系统没有任何关系。因为操作系统是创建在高级格式化的硬盘分区之上，是和一定的文件系统相联系的。

3. 恢复电脑上Win 7单系统的启动模式

要想重新启动电脑直接就能进入Win 7操作系统，就必须重新改写电脑硬盘上的MBR记录。电脑一般是在硬盘中划出几到几十兆的空间存放MBR记录，如图7-14所示。在H盘的后面有一个9M的未分配的空间，这里其实存放的就是MBR记录。进入到“计算机管理”中，在“9M未分配”上点击右键，选择“属性”，进入到“卷”中，就可以看到“磁盘分区形式：主启动记录(MBR)”，如图7-15所示。

图7-14　MBR位于硬盘中位置的图示

置”，出现如图7-16所示的对话框。在“默认操作系统(S)”中，选择以前的操作系统“Windows 7”，单击“确定”按钮。这样以后在重新启动电脑时，就可以自动的进入到以前的Win 7操作系统了，不再有选择要进入到哪个操作系统的界面，也不会有如图7-13所示的GRUB选择图示。这样既方便了用户快捷的登录到电脑的操作系统中，也节省了开机的时间。

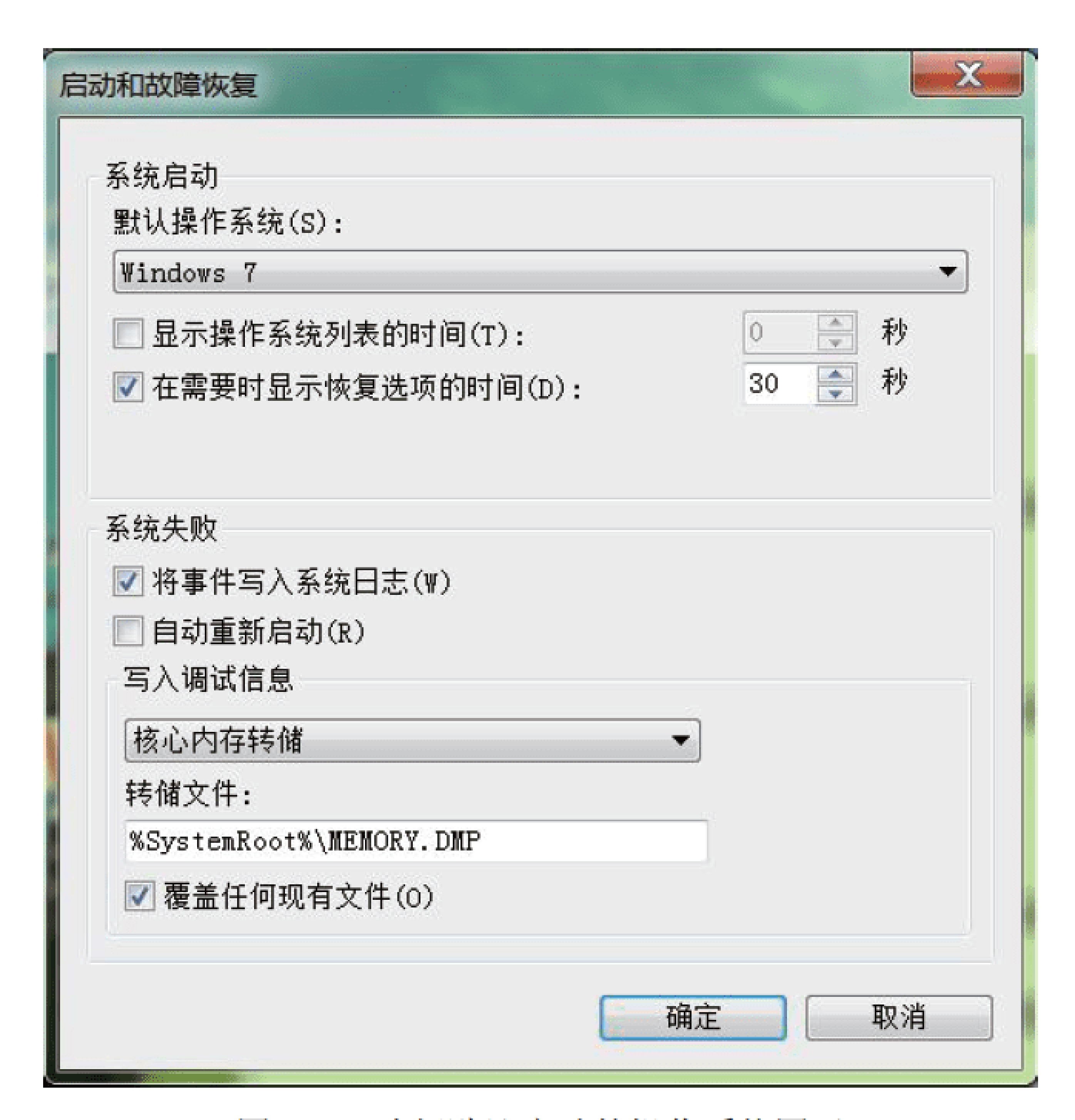


图7-16　选择默认启动的操作系统图示

4. 总结

(1)一般电脑在加电后，首先启动的是BIOS程序，BIOS自检完成后，找到硬盘上的主引导记录MBR，MBR读取DPT分区表，从中找出活动的主分区，然后读取活动主分区的PBR，PBR再搜寻分区内的启动管理器文件BOOTMGR，在BOOTMGR被找到后，控制权就交给了BOOTMGR。BOOTMGR读取\boot\bcd文件。其中，Win 7下的BCD(Boot Configuration Data，启动配置数据)文件就相当于Windows XP下的boot.ini文件，如果存在着多个操作系统，并且选择操作系统的等待时间不为0的话，这时就会在显示器上显示操作系统的选择界面。在选择启动Win 7操作系统后，BOOTMGR就会去启动盘寻找 WINDOWS\system32\winload.exe，然后通过winload.exe加载Win 7内核，从而启动整个Win 7操作系统。

对应的。VLAN中的PC都是通过Cisco3560接入到网络中，3560都是二层配置，三层的配置都在Cisco4507上，也就是VLAN间的路由都是通过4507完成的。PC的IP地址、默认网关和DNS都是自动从DHCP服务器上获得的，不用手工静态配置。

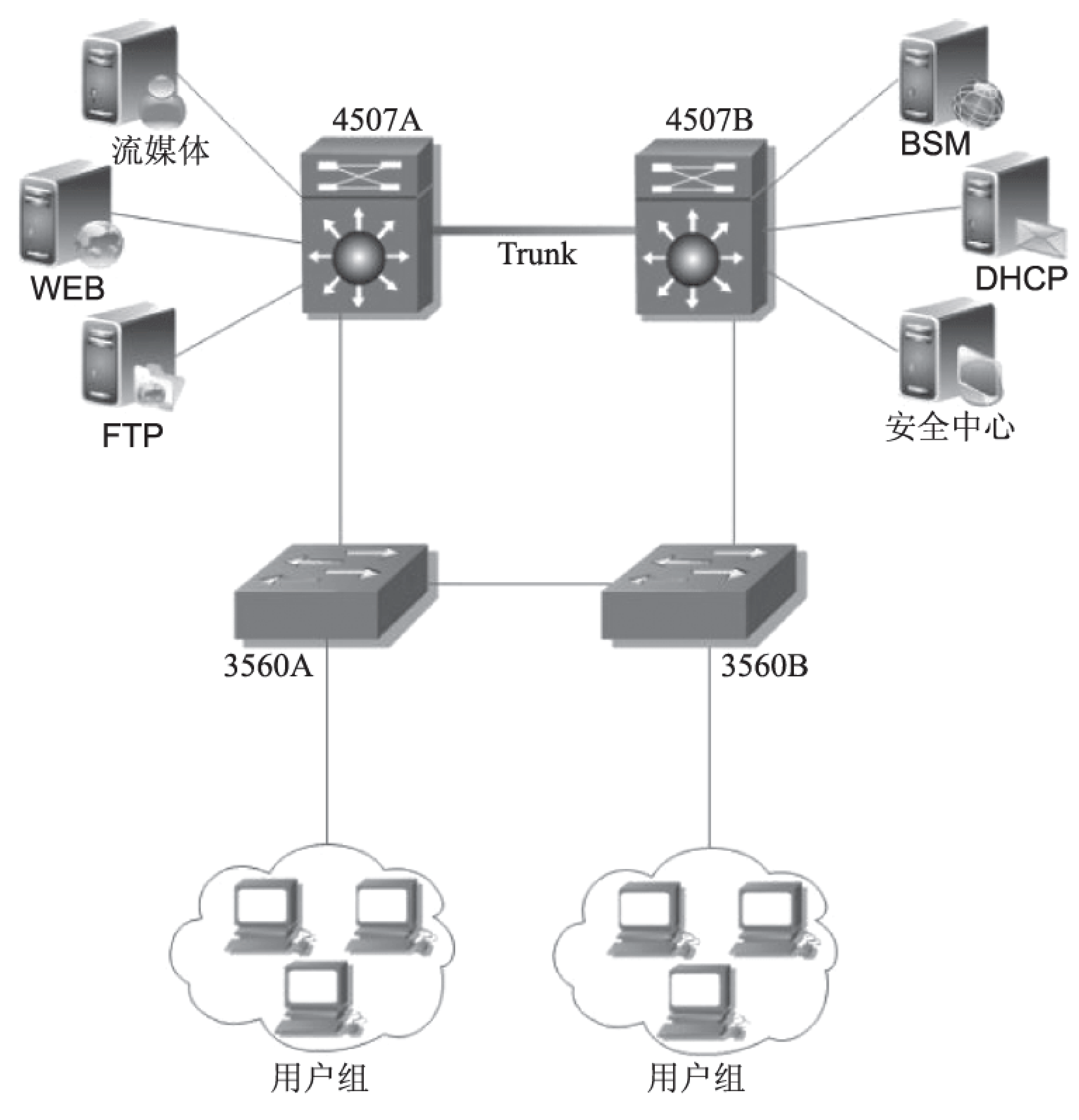


图7-17　网络结构图

7.3.2　故障发生过程

公司流媒体服务器位于VLAN 2中，IP地址为192.168.2.8/24。网络中有权限的用户可以进入到服务器中下载、上传和编辑一些视频剪辑。一天早上，业务网VLAN 12中的很多用户反映他们部门的人员都不能访问流媒体服务器，也不能进入服务器中流媒体应用系统的Web界面。

但是VLAN 12中的用户访问其他VLAN中服务器上的应用，都很正常，如都能正常访问VLAN 10中的WEB服务器。而且办公网和业务网中除了VLAN 12，

其他VLAN中的用户都能正常访问流媒体服务器，也就是只有VLAN 12中的用户访问不了。因为流媒体应用是单位业务中一项很重要的应用，若长时间不能用的话，可能会影响到公司业务正常运转，所以必须尽快排除故障。

7.3.3 运用BSM排查故障步骤

1. 故障信息收集

通过对故障现象的分析，确定了故障的大概示意图，如图7-18所示。不能访问流媒体服务器的用户IP地址的网络号都是192.168.12.0/24。他们访问流媒体服务器的路径先是到Cisco3560，通过Cisco4507，最后到达服务器。

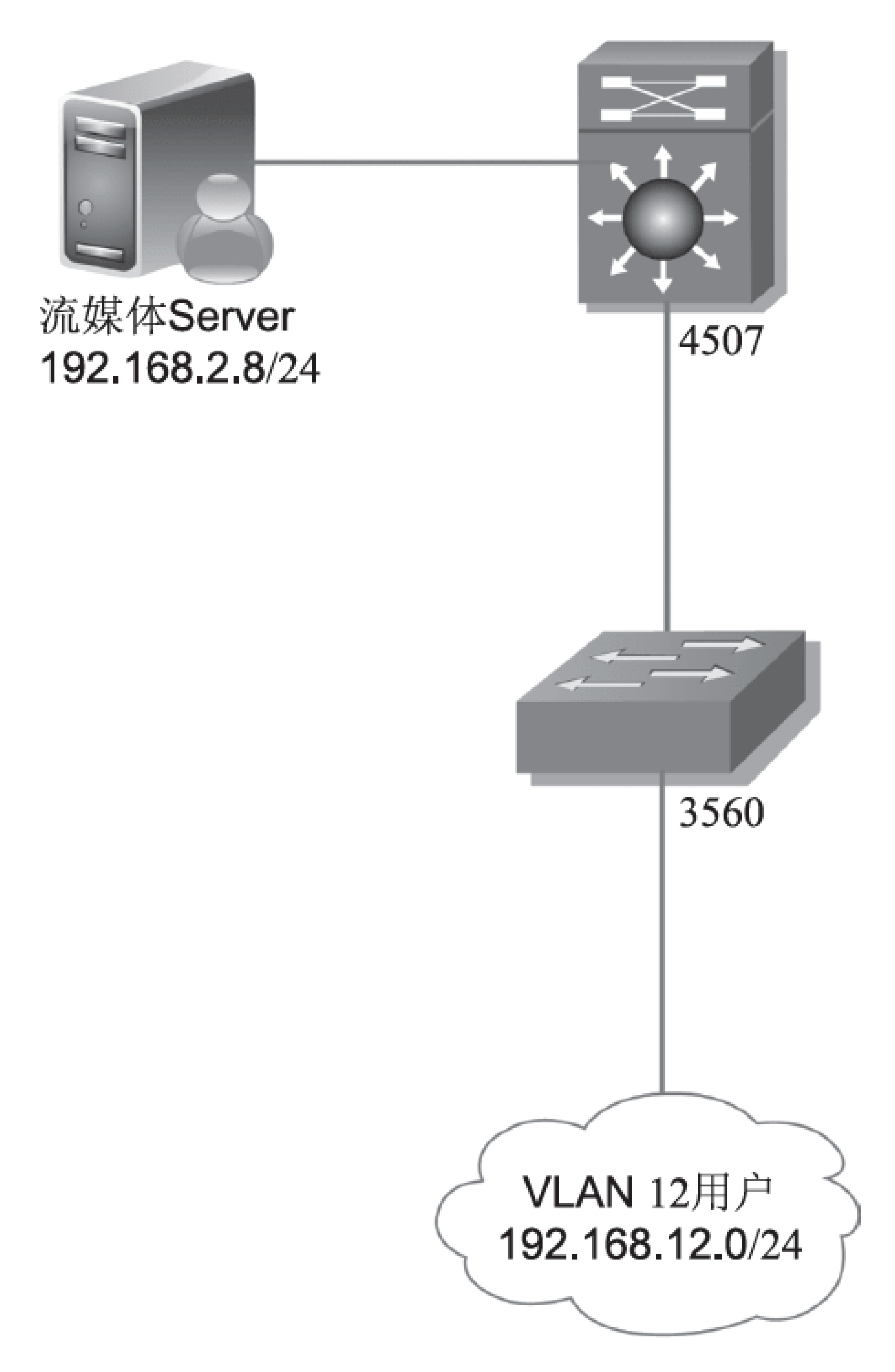


图7-18 存在故障的网络示意图

2. 客户端异常情况

我们到不能访问流媒体应用的部门，查看了用户的PC，发现电脑上的IP地址、默认网关、DNS都是正确的。然后我们在用户电脑的“命令行”中执行“ping 192.168.2.8”命令，结果ping不通。然后又执行了ping VLAN 12网关地址

的命令“ping 192.168.12.254”，发现能ping通。为了确定出具体的故障部位，又在“命令行”中执行了“tracert 192.168.2.8”命令，显示的结果如下所示：

```
C:\ >tracert 192.168.2.8

Tracing route to 192.168.2.8 over a maximum of 30 hops

1     <1 ms    <1 ms    <1 ms   192.168.12.254

2     *        *        *       Request timed out.

3     *        *        *       Request timed out.
```

从上面的结果可以看出，用户访问流媒体服务器时，数据包只能到达192.168.12.254，再往下路径就发生了故障，不能到达目的地。从前面的介绍知道Cisco3560上是没有IP地址配置的，它们都是作为二层交换机接入到网络中的，所有三层的地址都是在Cisco4507上配置的。也就是用户访问流媒体服务器的数据能到达4507，然后再往下就不知道哪出现了故障。可能是流媒体服务器故障，也可能是连接流媒体服务器和核心交换机4507之间的链路发生了故障。

3. 运用BSM排查故障

从上面的分析可以看出，故障很可能是流媒体服务器引起的。因为公司部署了BSM(Business Service Management，业务服务管理)，它能对公司所有的网络设备、服务器及业务应用系统的运行情况进行实时监控，所以通过使用“BSM业务服务管理”能够更快地查找出故障原因。

登录到BSM后，在“网络和服务器”拓扑图中的“流媒体服务器”图标上单击右键，就会出现如图7-19所示的选择菜单。在菜单中选择“接口一览”，就会出现如图7-20所示的显示界面。

在图7-20中能够显示出“流媒体服务器”上所有网络接口的主要情况，包括接口的IP地址、每个接口上的接收速率和发送速率。从图7-20中可以看出“流媒体服务器”上共有两个接口在传输数据，即eth0和eth2。其中eth0的IP地址为192.168.2.8，这个地址是单位用户访问流媒体服务器正常使用的IP地址。但在服

7.3.4 结束语

(1)作为IT运维人员，在工作中仅仅做好单台设备或单个应用的维护工作，已远远达不到全局保障单位IT系统正常运行的要求。而IT运维管理自动化技术的应用将会大大提高运维人员的工作效率。目前广泛使用的BMC Performance Manager和Mocha BSM产品都为企业的基础结构和关键业务应用提供了以业务为中心的智能化管理解决方案。

BMC Performance Manager解决方案允许用户对网络系统和众多的应用程序、数据库、操作系统和分布式系统环境的可用性、性能和业务影响进行监控和管理。通用的显示视图可以使IT管理员一览整体资源状态以及IT组件、应用服务对业务的影响。

BMC Performance Manager结合了无代理和基于代理的管理技术，简化了系统的安装与部署，主要面向对业务监控能力要求较高和对数据库监控能力要求严格的用户。采用基于策略的部署机制，可自动根据用户的环境和需求采用适当的管理技术。

(2)通常在计算机网卡、交换机和路由器的端口上都能配置两个或多个IP地址，在前两者上的主要作用是为了实现连接在同一局域网上不同网段之间的通信。一般由于一个网段中所包含的IP地址对于用户来说不够用，就可以采用配置多个IP地址的办法来扩大接入到局域网中用户的数量。而在路由器的端口上配置两个或多个IP地址主要是实现连在同一路由器端口的不同网段的通信，但这时要注意启用端口上的IP重定向功能，因为一般路由器不允许从同一端口进来的IP数据包又发回到原端口中。启用了重定向功能，就允许在同一端口进入路由器的IP数据包由原端口再发送回去。但是在计算机网卡、交换机和路由器的端口上配置多个IP地址常常会给网络带来意想不到的故障，所以一般没有特殊需求，不要在同一端口上配置多个IP地址。

(3)这次公司流媒体服务器的故障也是因为在故障的前一天晚上，负责流媒体应用系统软件开发的厂商在公司调试软件，因为软件测试的需要，要在流媒体服务器的网卡上临时再配置一个IP地址，技术人员就随便配置了192.168.12.18这

个地址。测试完成后，技术人员离开公司时忘了把这个IP地址删除，结果就导致了第二天早上的网络故障。

按照公司的规定，对机房服务器上每一步重要的操作，都要记录在服务器日志登记本上。完成操作后，要逐项查看登记本，是否把服务器恢复到了初始的正常状态。但因为双方的技术人员都没有严格执行机房管理规定，从而造成了意外的疏漏。看来IT运维无小事，必须从点滴做起，从我做起。

7.4 运维实例：BSM在企业IT运维中的应用研究

目前，在绝大多数公司和企业中，IT运维人员的地位和作用越来越受到重视。但是，受重视并不代表IT运维人员的工作量和工作难度有所降低。相反，随着信息化、网络化的迅速发展，应用系统的数量不断增多，运维人员的劳动负荷也不断增大。但通常他们所做的工作都是一些重复、简单、繁杂的工作，效率低下。所使用的监控工具配备不完善，没有中间件、数据库和语音系统，也没有集中的事件管理平台，通常对故障不能及时发现和定位。

7.4.1 BSM基本功能

业务服务管理(BSM，Business Service Management)的使用可以极大地减轻IT运维人员的工作量，并提高了工作效率。BSM是IT与业务管理手段的一种整合与互补。它以ITIL为理论基础，实现IT管理与业务服务的融合。能够从不同监控系统整合出需要的IT营运信息，从而给企业带来IT服务方面的优势，进一步增强了企业竞争力。

从图7-23中可以看出BSM所具备的基本功能，主要包括6个方面：整合、用户体验响应时间管理、全方位管理、无线运维、可视化管理和网络拓扑。运维人员通过这6个功能，就能在日常工作中做到可视化、全方位管理，把故障消除在预防阶段，做到随时随地地了解设备运行情况等。

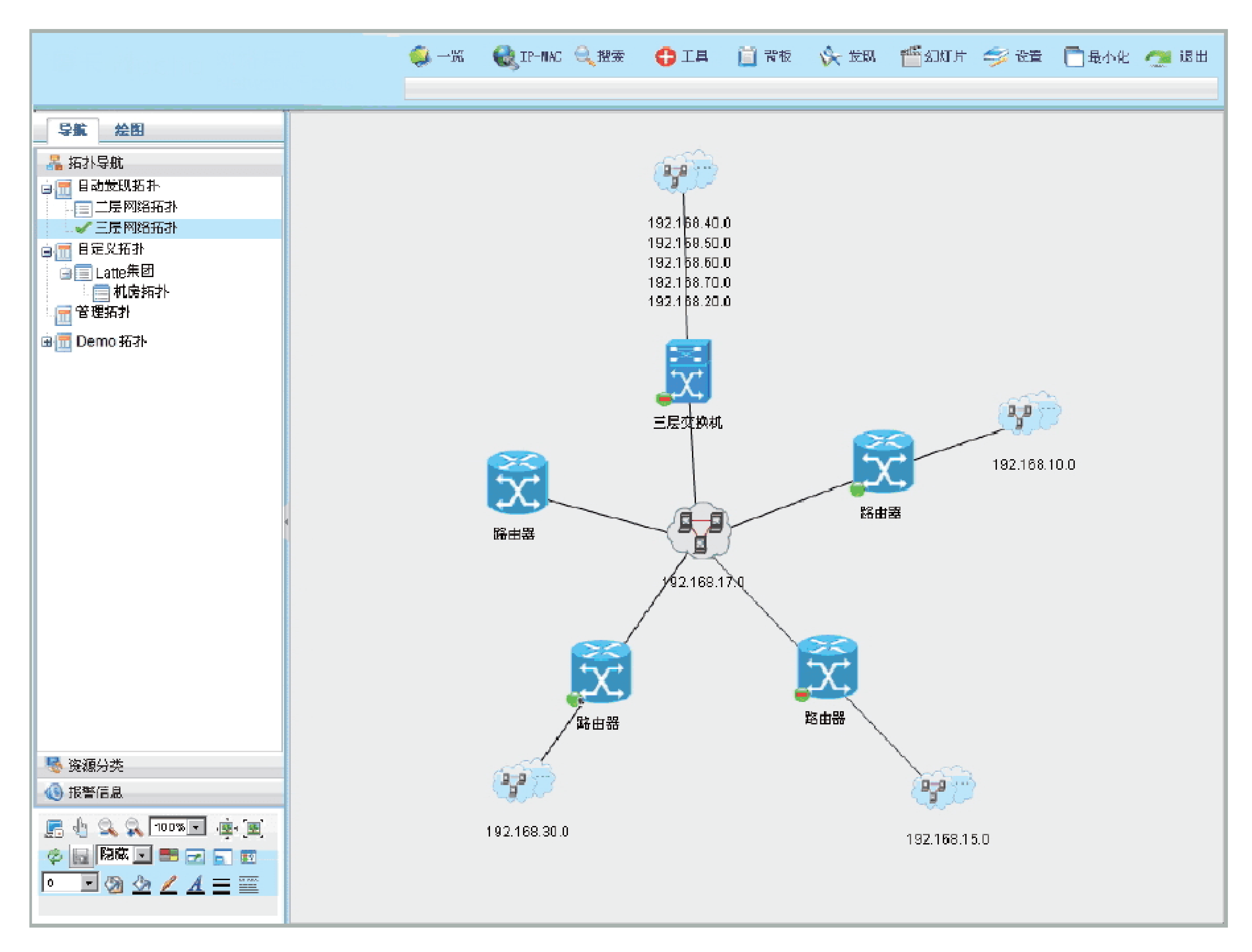


图7-24　网络拓扑图

而且，直接在拓扑图的设备图标上单击右键，在出现的菜单中可以选择相应的网络检测工具，如“Ping”和“Telnet”工具，通过使用检测工具能够更准确地定位故障的部位和查找故障的原因。

2. 网络设备详情

通过查看网络设备详情，可以看到设备目前的常规信息：设备类型、IP地址、持续运行的时间和资源总体状态等。在常规信息中还可以看得到设备的维护信息(包括责任人、责任人的联系电话和电子邮件)、设备备注情况、设备的CPU和内存使用情况等，如图7-25所示。

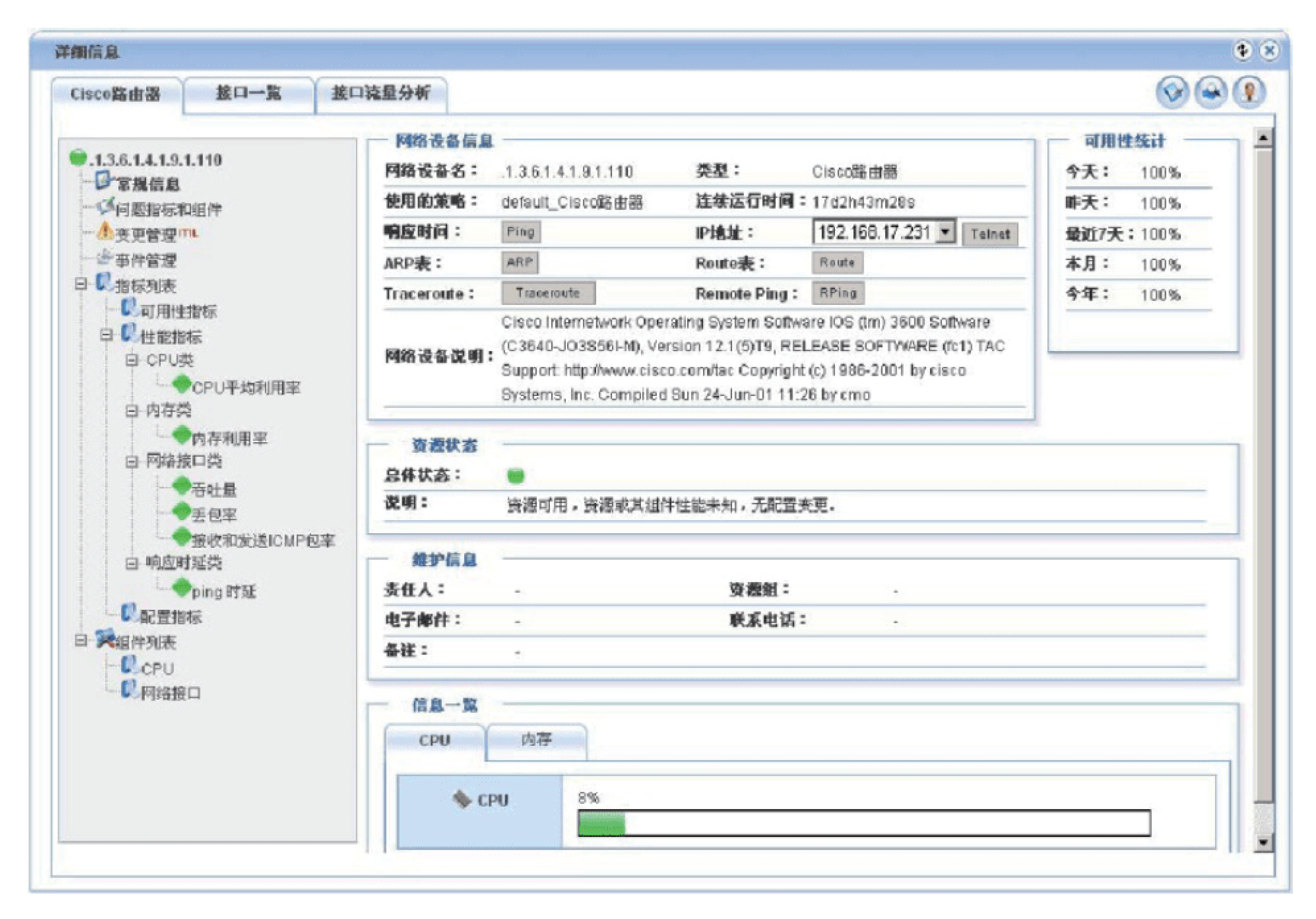


图7-25　网络设备详情

在网络设备详情中，还可以看到网络设备的每一个接口的实时速率、接口状态是否良好、故障接口的图标颜色会变成红色进行报警、良好的接口会以绿色显示以及每个接口到目前为止的数据流量是多少。网络设备详情中还可以展现当前网络设备所有被监控的接口流量信息，并对单个接口的流量以及多个接口对比的流量做实时分析，能够更全面和深入地了解到网络设备和每一个端口的使用情况。

3. 主机系统详情

在主机系统详情中的常规信息中可以看到主机信息、可用性统计、资源状态、状态一览、维护信息及CPU、内存、硬盘等信息的情况，如图7-26所示。

常规信息中的“使用的策略”是显示主机当前使用的策略名称。由系统管理员在‘策略管理’中设置。在策略中需要设置该主机监控的指标、指标阈值、监控频度、事件、报警等参数；“用户域”显示主机所属的所有用户域；“响应时间”可以单击 ping 按钮，获取主机的响应速度；“Telnet”单击Telnet 按钮，出现命令窗口，本地主机将与远程主机建立连接。使用 Telnet 协议进行远程登录时，在本地计算机上必须装有包含Telnet 协议的客户程序，必须知道远程主机的

IP 地址或域名，必须知道登录标识与口令；“网络链接”单击 Netstat 按钮，可以打开主机上的端口列表情况；“主机说明”是由系统自动获取的主机说明信息。

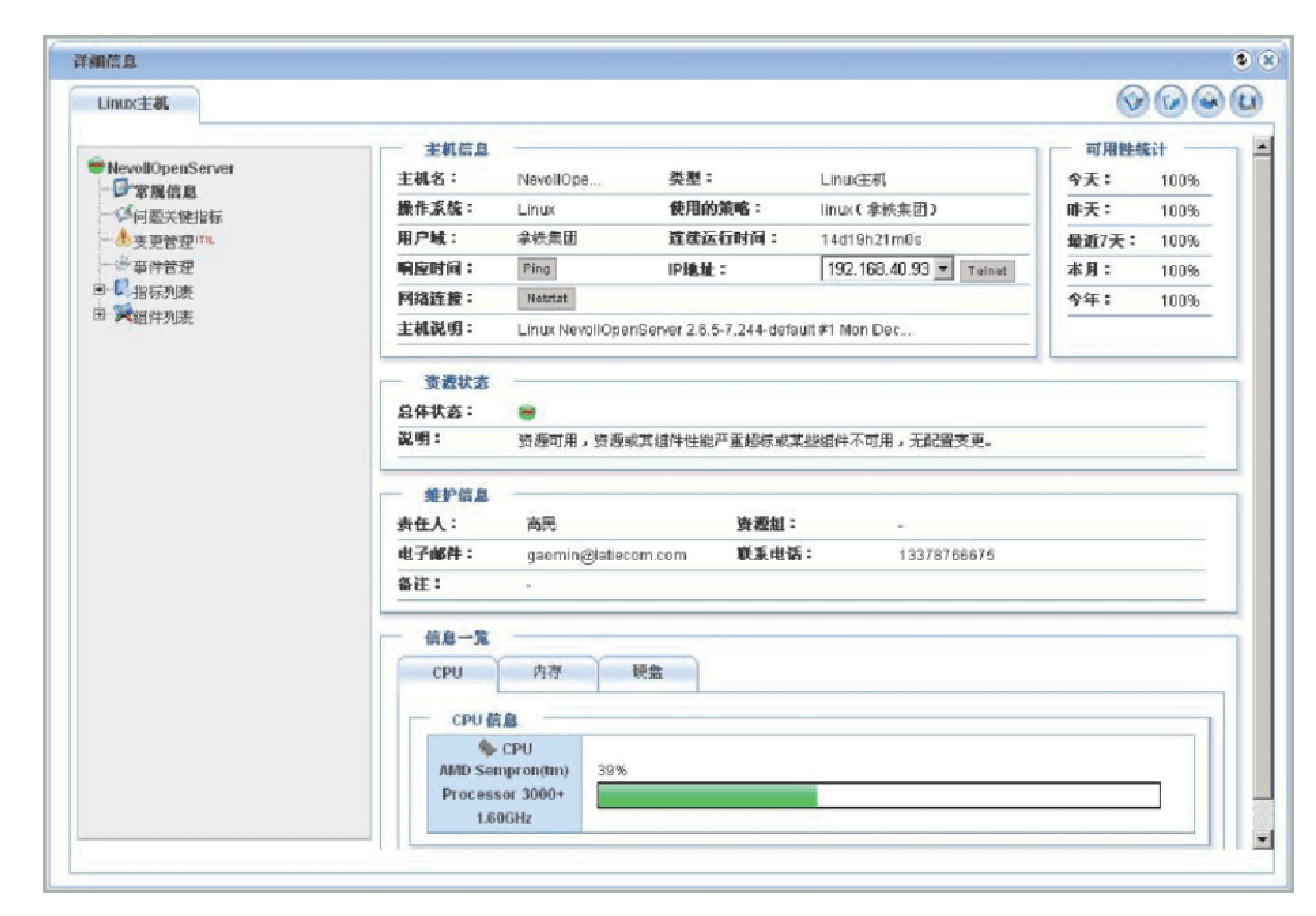


图7-26　主机系统详情

常规信息中的“可用性统计”是按时间段统计主机的可用性比率；“资源状态”是对所有资源的状态进行说明；“维护信息”是由系统管理员在系统管理的资源中进行设置显示的；“信息一览”展示CPU、内存、硬盘的信息，只有在策略中配置了监控CPU、内存、硬盘的相关指标，这里才会显示。“CPU 信息”显示了CPU型号、主频、CPU平均利用率。“内存信息”显示了内存总容量、内存平均利用率。“分区信息”显示了分区总容量、各分区容量和利用率。

4. 主机进程管理

主机进程管理可以看到当前主机上运行的所有进程及进程的详细信息，也可以大概看出主机上是否有木马、流氓软件、广告软件等在运行。因为一个运行的程序是否正常，主要看它对应的是正常的程序文件，还是恶意木马。从对应文件目录或者文件名上可以分析出这个程序的主要作用，而对于不熟悉的文件，可以通过查询资料了解它是否是正常程序。例如在Windows系统中的WINDOWS目录

状况，通过输入IP地址或者资源名称，定位到需要查看的资源，并且搜索功能支持模糊查询。如图7-28所示。

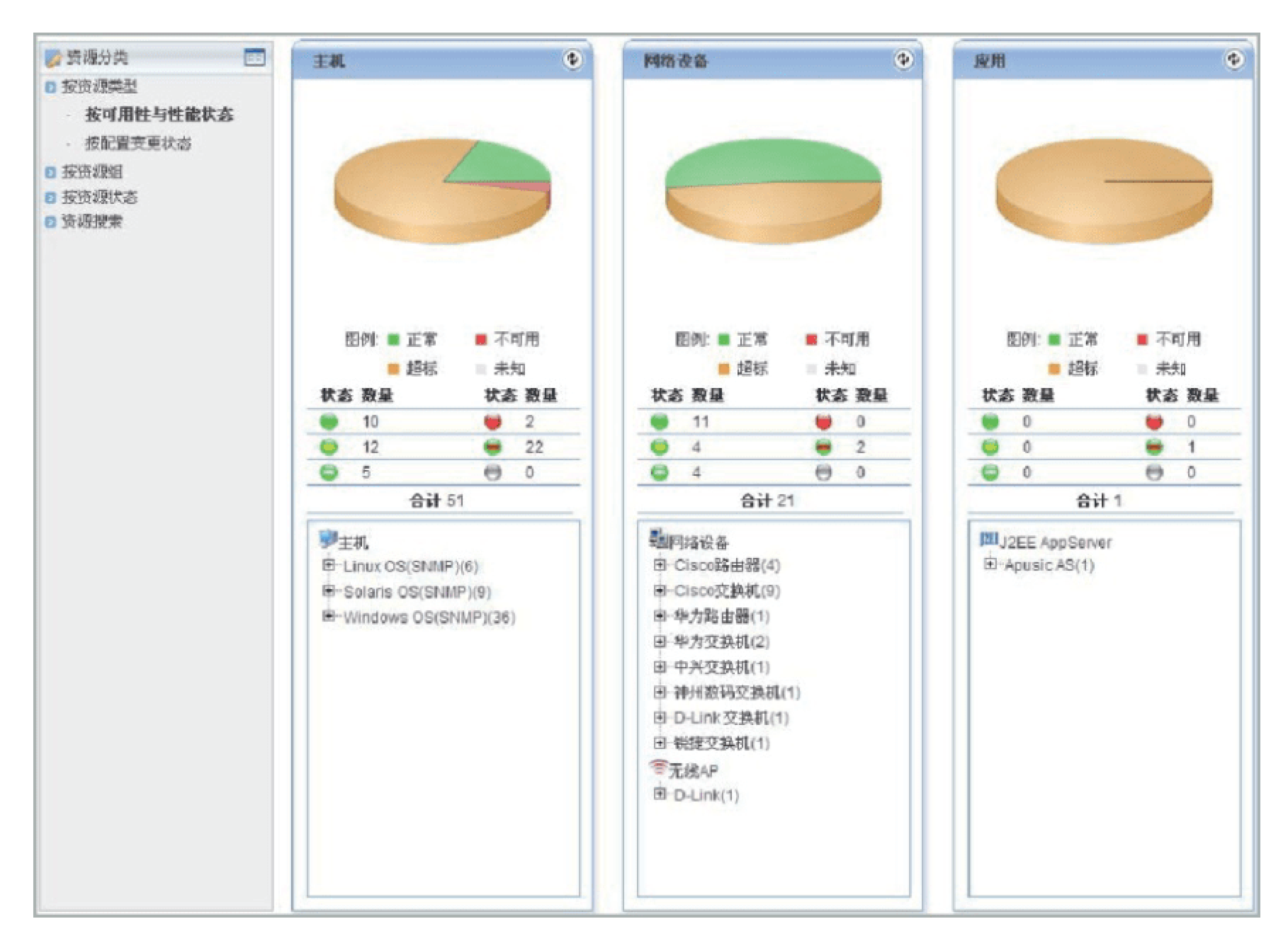


图7-28　资源监控管理

(1)按资源类型查询资源状态。可以从两种角度查看资源的总体情况：按可用性与性能状态展现或者按配置变更状态展现。按可用性和性能状态展现，只关心资源的可用性和性能状态，不关心资源的配置变更；按配置变更状态展现，只关心资源的配置变更状态，不关心资源的可用性和性能状态。

资源类型包括主机、网络设备和应用。将鼠标放到饼图某一颜色的区域上，会显示提示信息。单击资源名称可以进入资源详细信息页面；单击资源名称前的状态灯可进入状态信息页面。

(2)按资源组查询资源状态。左侧导航区域中会列出所有资源组的名称。单击资源组名称，右边信息展示区会显示相应的资源；以饼图的方式展示资源组中被监控资源的总体状况。

(3)按资源状态查询资源。以资源的5种可用性、性能、配置状态为单位，显示这5种状态的资源的状况。单击左侧导航区域中的“按资源状态”即可。

将鼠标放到饼图某一颜色的区域上，会显示提示信息；饼图下方，显示处于

相对BSM要简单许多，所以对IT运维人员进行培训也是必不可少的。

培训主要包括三方面内容的培训：一是管理人员的培训，主要是BSM监控系统的使用方法和注意事项及当BSM发出故障报警时的事件处理流程。二是网络部门人员的培训，包括网络拓扑图建立、修改和删除的方法步骤和在交换机、路由器等网络设备上配置参数的方法。三是主机应用系统人员的培训。包括在BSM中添加服务器的方法和步骤及在不同操作系统Windows、Linux、Unix和Solaris中配置参数的方法。

7.5.1　BSM在企业中应用后的效果

BSM在企业中的部署应用，不仅减轻了IT运维人员的工作量，也提高了业务部门人员的工作效率。它给企业带来的增值效益主要体现在以下几方面：

一是BSM的短信、邮件报警机制缩短了IT运维人员排除故障的时间。因为在没有部署BSM之前，IT运维人员得到设备故障的反馈信息，大多数都是从使用应用系统的工作人员那里得到的。例如，从用户那里反映过来的网络故障，某个应用系统不能使用等。IT运维人员在得到用户的反馈后才去排查、定位故障发生的部位。但是部署了BSM的短信、邮件报警机制后，设备或应用系统出现故障的第一时间，IT运维人员就能通过短信或邮件得到故障的信息和故障的部位，这就在很大程度上提高了IT运维效率。

二是全局监控网络和应用系统，快速准备定位故障部位。在没有部署BSM前，企业的网络和应用系统监控是隔离开的，各监控各的。部署BSM后，可以把二者的监控紧密结合起来。也就是在拓扑图中，既有网络设备，又有应用系统的服务器设备。这种机制能够快速定位故障发生的部位。例如，当有用户反映某一应用系统不能正常使用时，IT运维人员只需通过拓扑图，查看是应用系统服务器故障，还是服务器连接的网络设备故障，若有故障，这些设备在拓扑图中的图标颜色都会变成红色，所以很快就能定位到故障发生的位置。

三是提前预警机制，把隐患消除在了萌芽阶段。IT运维人员可以对设备的某一参数设置一个阀值，当设备的某些数据达到这一阀值时，但设备还没有故障之前，BSM会自动给运维人员进行报警。这样IT运维人员就有足够的时间对设备

进行维护和排除故障，这一过程不会对正常使用业务应用系统的用户造成任何影响。

7.5.2 总结

虚拟化和云计算已是目前绝大多数企业在进行信息化建设时的首选。但是二者的深入应用都离不开IT基础设施的保驾护航。所以，担负IT基础设施监控管理的BSM就越发显得责任重大。虚拟化和云计算的广泛应用，进一步把企业信息化系统中的软、硬件紧密结合起来。因为在一台服务器中可能会虚拟出多个应用系统，这些应用系统间有的有数据交互，有的没有，这种模式和传统的应用模式已大大不同。在这种情况下就更需要企业部署BSM系统，以便全局监控管理企业信息化中的每一个细节。所以，BSM系统也越来越成为企业信息化建设中不可缺少的重要一员。

第8章 排查工具应用

```
Cisco3750(config-if)#switchport mode access
//把Cisco3750端口Gi1/0/1划入到VLAN 21
Cisco3750(config)#interface GigabitEthernet1/0/9
Cisco3750(config-if)#switchport access VLAN 31
Cisco3750(config-if)#switchport mode access
//把Cisco3750端口Gi1/0/1划入到VLAN 31
```

Cisco3750上启用了三层路由功能，这样不同VLAN中的数据终端要相互通信的话必须经过3750路由后，数据才能传输到目的地。例如，图8-1中位于VLAN 21中的PC 1要访问VLAN 31中的PC 2，那PC 1发出的数据包就先要到达Cisco3750的三层VLAN 21端口，然后3750查找它的路由表，发现数据包的目的地址是要到达VLAN 31，根据路由表中的下一条地址，它就把数据包发送到3750上的三层VLAN 31端口，最后到达目的终端。

3)问题发生过程

其实，从事网络工作的同志对图8-1的网络结构和在交换机上所做的配置命令都是很常见的情况，也是网络配置中最基础的。所以当自己在这种网络结构中碰到ping故障时觉得非常奇怪，因为觉得不应该有这种故障情况。也就是在图8-1中PC 2能ping通PC 1，但是PC 1不能ping通PC 2。

数据包从PC 1发出，最终到达PC 2的路线也非常简单，首先是从PC 1的网卡把数据包发出，数据包到达VLAN 21的三层口上，然后Cisco3750再把数据包交给VLAN 31的三层口，最后一步就是VLAN 31三层口把数据包传输给都位于同一个二层VLAN 31的PC 2上的网卡即可。因为成功的一次ping过程都是有去有回的，所以从PC 2返回到PC 1的ping数据包也就是沿着上面所述路线的反方向返回即可。而且，通常是A能ping通B的情况下，B也就能ping通A。所以这种故障是比较奇怪。

4)问题解决过程

(1)首先考虑到的是不是Cisco3750上的路由引起的故障。所以就把PC 1和PC 2两台电脑放置到同一个VLAN中，这样两台PC之间的ping包就不用通过路由传

输。但是放置在同一个VLAN中后，上面的故障现象依旧，也就说明故障不是由Cisco3750上的路由引起的。

(2)既然不是Cisco3750上的路由引起的，那很可能故障就发生在两台PC上。因为连接两台PC和Cisco3750之间的两条网线一般不会引起这种ping故障。所以就另外找了一台笔记本电脑PC 3，用它替代了PC 1的位置，而且让PC 3和PC 1上的网络参数配置完全一样，但是故障现象依旧。到这一步也就排除了故障发生在PC 1上的可能性。

(3)既然故障不在Cisco3750和PC 1上，所以故障很有可能就出在PC 2上。用PC 3替换了PC 2的位置，同时调整PC 3上的网络参数，让它和PC 2上的参数完全一样。结果发现故障现象消失，PC 1能ping通PC 3，PC 3也能ping通PC 1。所以到这一步就能确定故障就发生在PC 2上了。

(4)在上面排查故障的过程中，PC 1和PC 3两台电脑上安装的操作系统都是Windows XP系统，但PC 2上使用的是Win 7操作系统，难道和操作系统有关？后来想到微软在开发Win 7时，把操作系统的安全性又进行了提升。而且常常微软操作系统的防火墙功能会引起一些莫名其妙的故障，所以故障很有可能就出在Win 7的防火墙上。

在PC 2电脑的“控制面板”→“所有控制面板项”→“Windows 防火墙”→“自定义设置”中，发现Win 7操作系统“家庭或工作(专用)网络”和“公用网络”两个网络的防火墙功能都是打开的，如图8-2所示。



图8-2　PC 2上的防火墙处于开启状态

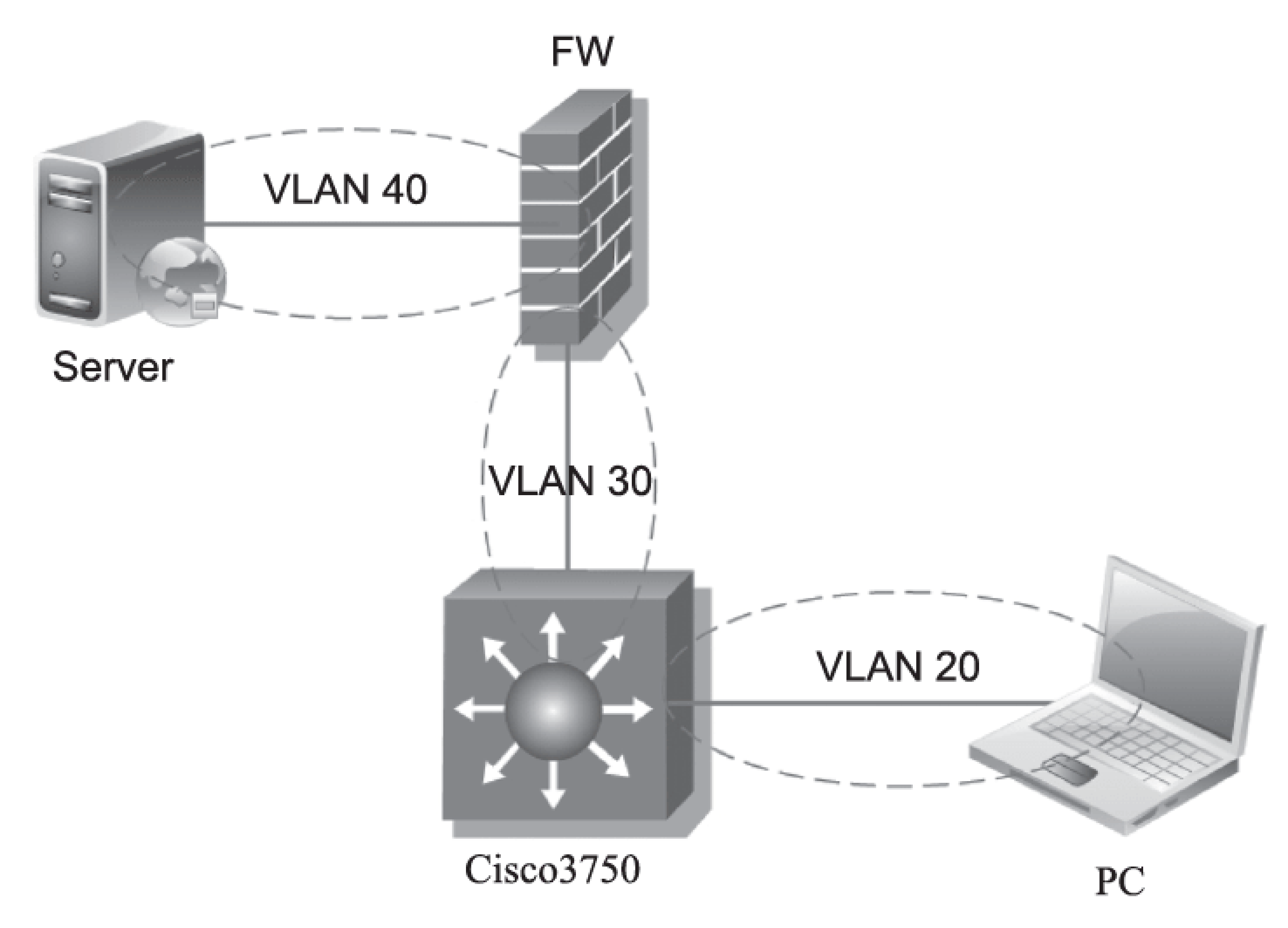


图8-4　Ping实例二网络结构图

2)交换机上主要配置

网络设备Cisco3750上的具体配置命令如下所示：

```
Cisco3750(config)interface VLAN 20
Cisco3750(config-if)ip address 192.168.20.254 255.255.255.0
//配置Cisco3750三层VLAN 20的IP地址
Cisco3750(config)interface VLAN 30
Cisco3750(config-if)ip address 192.168.30.254 255.255.255.0
//配置Cisco3750三层VLAN 30的IP地址
Cisco3750(config)#interface GigabitEthernet1/0/1
Cisco3750(config-if)#switchport access VLAN 20
Cisco3750(config-if)#switchport mode access
//把Cisco3750端口Gi1/0/1划入到VLAN 20
Cisco3750(config)#interface GigabitEthernet1/0/2
Cisco3750(config-if)#switchport access VLAN 30
```

```
Cisco3750(config-if)#switchport mode access
//把Cisco3750端口Gi1/0/2划入到VLAN 30
Cisco3750(config)#ip route 192.168.40.0 255.255.255.0 192.168.30.1
//在Cisco3750上配置到网络192.168.40.0/24的路由
```

3)问题发生过程

从图8-4中可以看出，在电脑PC上ping服务器Server的数据包传输总共进行了一次路由，也就是在Cisco3750上进行了路由。

在PC上的ping包首先通过网卡传输到Cisco3750交换机的G1/0/1端口上，交换机发现ping包所要到达的目的地不是在它所连接的网络中，然后通过查找路由表(ip route 192.168.40.0 255.255.255.0 192.168.30.1)，把ping数据包传输给FW的GigabitEthernet 1端口。防火墙收到ping数据包后，发现ping包所要到达的目的地正是端口GigabitEthernet 2所连接的VLAN 40网段，所以它就直接在VLAN 40中进行了广播，最终服务器Server也就收到了ping包。

在PC上ping服务器Server返回的数据包路线正好和上面所述的路线相反。按说从PC上能ping通Server，那么从Server上也就能ping通PC，因为它们的数据包所走的路线都是一样的。但事实并非如此，在图8-4所示的实例中，PC能ping通Server，但在Server上却不能ping通PC。

4)问题解决过程

(1)因为从服务器Server上ping电脑PC也要经过3个网段：VLAN 40、VLAN 30和VLAN 20。对照数据包传输的路径一个个检查，先在Server上ping防火墙的GigabitEthernet 2端口，它和Server的网卡口都位于VLAN 40中，结果能ping通。然后再在服务器Server上ping交换机Cisco3750的G1/0/2端口，此端口位于VLAN 30中，也是从Server上发送ping包所要经过的端口，结果能ping通。

(2)从上面(1)中可以看出从Server到防火墙FW和交换机Cisco3750的网络都是通的。所以可以断定从Server上ping不通PC就是ping数据包到达Cisco3750上后，不能再经过VLAN 20把数据包传输给电脑PC。造成这种问题最大的可能就是在防火墙FW上没有进行正确的路由配置导致的。

(3)登录到防火墙设备上，查看设备上的路由配置，如表8-1所示。

表8-1　防火墙FW上的路由配置

序号	目的IP地址	目的IP地址子网掩码	下一跳地址
1	192. 168. 2. 0	255. 255. 255. 0	192. 168. 30. 254
2	192. 168. 3. 0	255. 255. 255. 0	192. 168. 30. 254
3	192. 168. 17. 8	255. 255. 255. 255	192. 168. 30. 254
4	192. 168. 4. 0	255. 255. 255. 0	192. 168. 30. 254
5	192. 168. 12. 0	255. 255. 255. 0	192. 168. 30. 254
6	192. 168. 10. 9	255. 255. 255. 255	192. 168. 30. 254

从上面防火墙FW上的路由表可以看出，没有到达目的网络“192.168.20.0/24”的路由，所以当从服务器Server上ping电脑PC的数据包到达防火墙后，FW找不到对应的路由就把ping包丢弃了，自然ping包也就传输不到电脑PC了。

(4)在防火墙FW上添加路由“ip route 192.168.20.0 255.255.255.0 192.168.30.254”，也就是防火墙FW收到要到达网络“192.168.20.0/24”的数据包后，都把它传输到Cisco3750的VLAN 30的三层端口(IP地址为192.168.30.254)上。添加路由后服务器Server也能成功ping通PC了。

3. 总结

(1)以上两个实例都推翻了网络运维工程师常犯的一个错误：总认为“A和B两个终端，A能ping通B，B就肯定能ping通A”。在实例一中是因为Win 7操作系统的防火墙，在实例二中是因为防火墙FW的原因，而导致两个终端之间不能互相ping通。这也说明在目前的互联网环境中，随着安全问题的日益突出，安全产品的使用数量也越来越多，而每个安全产品的设计和工作理念都不一样，这就给我们网络运维工程师带来了巨大挑战。要求在工作中，一定要针对每一个故障现象和细节问题认真分析、深入思考，这样才能真正排除掉网络系统中的安全隐患。

(2)通过深入分析“ping故障实例二”，我们还能发现有一个细节问题，就是电脑PC发出ping服务器Server的数据包，按照Cisco3750和防火墙FW上的路由配置，它是能够到达Server上的，但是每个ping包都是一个环路，有去有回的。那当从Server返回的ping包，它是怎么到达PC的，因为在防火墙FW上并没有配置到PC所在VLAN 20的路由。

这其实也涉及到目前绝大多数防火墙产品在设计上的一个理念，那就是防火墙的“记忆”功能。也就是当PC发出ping服务器Server的数据包后，它能记住ping数据包来时的路线。然后，当防火墙FW再次收到从Server返回的数据包后，它能把数据包按照自己起初记忆的线路，再沿着反方向把数据包从指定的端口传送出去。所以，网络运维人员若是没有理解这点的话，也是很难明白防火墙的工作过程。

(3)PING(Packet Internet Grope)，因特网包探索器，是DOS命令，可以检查网络的连通性，能够很好地分析判定网络故障。ping命令还可以结合多个参数使用，只要键入ping按回车即可看到各个参数的详细说明。但是某些病毒木马会强行大量远程执行ping命令抢占网络资源，导致系统、网速变慢。所以，许多操作系统把严禁ping入侵作为大多数防火墙的一个基本功能提供给用户进行选择。通常的情况下如果电脑不用作服务器或进行网络测试，就可以禁用ping功能，从而达到保护电脑的目的。一般执行ping命令，得到的反馈信息有以下几种情况：

①Request timed out(请求超时)。收到此类反馈信息一般是由四种情况造成：一是对方已关机，或者网络上根本没有这个地址。二是对方与自己不在同一网段内，通过路由也无法到达对方，但有时对方确实是存在的，当然不存在也是返回超时的信息。三是对方确实存在，但设置了ICMP数据包过滤。不过，要想知道对方是存在，还是不存在？可以用带参数“-a”的ping命令探测对方，如果能得到对方的NETBIOS名称，则说明对方是存在的，是有防火墙设置，如果得不到，多半是对方不存在或关机，或不在同一网段内。四是设置了错误的IP地址。正常情况下，一台主机应该有一个网卡、一个IP地址、或多个网卡、多个IP地址。若是多个IP地址的话，这些地址一定要处于不同的IP子网。但如果一台电脑在网络适配器的TCP/IP配置中，设置了一个与另外一个网卡的IP地址相同的子网中，这样在IP层协议看来，这台主机就有两个不同的接口处于同一网段内，同样也会导致ping超时的后果。

②Destination host Unreachable(目的主机不可达)。当对方与自己不在同一网段内，而自己又未设置默认的路由，就会出现此种信息提示。“Destination host Unreachable”和“Time out”还是有区别的，如果所经过路由器的路由表中具有到达目标的路由，而目标因为其他原因不可到达，这时候就会出现“time out”。如果路由表中连到达目标的路由都没有，就会出现“destination host

unreachable”。

③Unknown host(不知名主机)。这种出错信息的意思是，该远程主机的名字不能被域名服务器DNS转换成IP地址。故障原因可能是域名服务器故障，或者其名字不正确，或者网络管理员的系统与远程主机之间的通信线路有故障。

④No answer(无响应)。这种故障说明本地系统有一条通向中心主机的路由，但却接收不到它发给该中心主机的任何信息。故障原因可能是中心主机没有工作，本地或中心主机网络配置不正确，本地或中心的路由器没有工作，通信线路有故障，或中心主机存在路由选择问题等。

(4)Win 7操作系统安全性。“ping故障实例一”就是因为Win 7中的防火墙设置不正确而引起的。Win 7操作系统不但改进了安全和功能的合法性，而且把数据的保护和管理扩展到了外围设备。还改进了基于角色的计算方案和用户账户管理，在数据保护和坚固协作的固有冲突之间搭建了沟通桥梁，同时也开启了企业级的数据保护和权限许可。

在Win 7以前的操作系统中，一般也有自带的防火墙，但功能简单，一般被视为鸡肋。而Win 7的防火墙做了很大改进，在功能上更加强大。它最大特点是内外兼防，通过“家庭或者工作网络”和“公用网络”两个方面来对计算机进行防护。尤其是“高级设置”里面功能更加全面，可以与一般的专业防火墙软件相媲美，通过入站与出站规则可以设置应用程序访问网络的情况。另外监视功能可以清晰反映出当前网络流通的情况，还可以设置自定义的入站和出站规则。

8.2　运维实例：两则Telnet故障排查实例

网络结构图如图8-5所示。为了确保重要设备的稳定性和冗余性，核心层交换机使用两台Cisco4506，通过Trunk线连接。在汇聚层和接入层分别使用了多台Cisco3750、Cisco3560交换机，图示为了简洁，都只画出了两台。单位IP地址的部署，使用的是C类私有192网段的地址。Cisco4506和Cisco3750之间以及Cisco3750和Cisco3560之间都是Trunk连接。

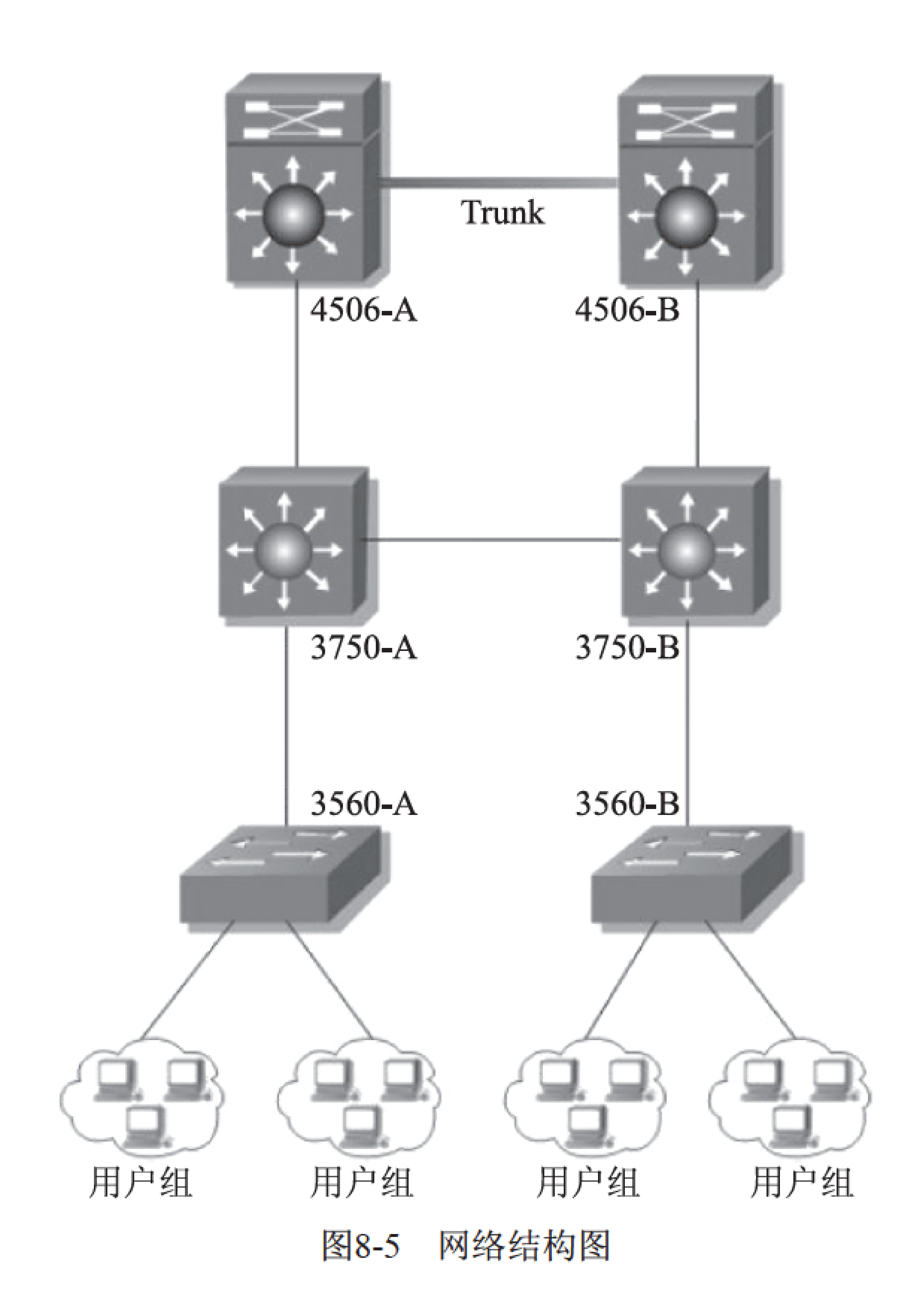


图8-5　网络结构图

根据部门性质的不同，把不同部门划入到不同的VLAN中。服务器都部署于VLAN 5～VLAN 10中，对应的网络号是192.168.5.0～192.168.10.0，如FTP服务器位于VLAN 5中。服务器的IP地址、默认网关和DNS都是静态配置的。VLAN 11～VLAN 200是属于各个部门使用，对应的网络号是192.168.11.0～192.168.200.0。VLAN号和网络号之间都是对应的。VLAN中的PC连接到Cisco3560，通过Cisco3750接入到核心交换机。Cisco3750和Cisco3560都是二层配置，三层的配置都在Cisco6506上，也就是VLAN间的路由都是通过6506完成的。PC的IP地址、默认网关和DNS都是自动从DHCP服务器上获得的，不用手工静态配置。

1. Telnet故障实例一

如图8-6所示，是Telnet故障实例一所涉及到的网络部分。设备间的连接情况如下所示：

```
Cisco4506 GigabitEthernet 3/1  <-----> Cisco3750
```

```
//配置Cisco4506端口Gi3/1为Trunk模式
Cisco4506(config)interface VLAN 2
Cisco4506(config-if)ip address 192.168.2.254 255.255.255.0
//配置Cisco4506的VLAN 2的IP地址
Cisco4506(config)interface VLAN 11
Cisco4506(config-if)ip address 192.168.11.254 255.255.255.0
//配置Cisco4506的VLAN 11的IP地址
```

在Cisco3750上的配置命令如下所示：

```
Cisco3750(config)#interface GigabitEthernet1/0/1
Cisco3750(config-if)# switchport trunk encapsulation dot1q
Cisco3750(config-if)#switchport trunk allowed VLAN all
Cisco3750(config-if)#switchport mode trunk
//配置Cisco3750端口Gi1/0/1为Trunk模式
Cisco3750(config)#interface GigabitEthernet1/0/25
Cisco3750(config-if)# switchport trunk encapsulation dot1q
Cisco3750(config-if)#switchport trunk allowed VLAN all
Cisco3750(config-if)#switchport mode trunk
//配置Cisco3750端口Gi1/0/25为Trunk模式
Cisco4506(config)interface VLAN 2
Cisco4506(config-if)ip address 192.168.2.2 255.255.255.0
//配置Cisco3750管理IP地址
```

在Cisco3560上的配置命令如下所示：

```
Cisco3560(config)#interface GigabitEthernet1/0/1
Cisco3560(config-if)# switchport trunk encapsulation dot1q
Cisco3560(config-if)#switchport trunk allowed VLAN all
Cisco3560(config-if)#switchport mode trunk
//配置Cisco3560端口Gi1/0/1为Trunk模式
Cisco3560(config)#interface GigabitEthernet1/0/24
Cisco3560(config-if)#switchport access VLAN 2
Cisco3560(config-if)#switchport mode access
//把Cisco3560端口Gi1/0/24划入到VLAN 2
```

Cisco4506交换机上启用了三层路由功能，这样不同VLAN中的数据终端要相互通信的话必须经过4506路由后，数据才能传输到目的地。例如，位于VLAN 11中的PC要访问VLAN 2中的终端，那PC发出的数据包就先要到达Cisco4506的三层VLAN 11端口，然后4506查找它的路由表，发现数据包的目的地址是要到达VLAN 2，根据路由表中的下一条地址，它就把数据包发送到4506上的三层VLAN 2端口，最后到达目的终端。Cisco3750和Cisco3560都是二层配置，没有启用它的三层功能，也就是三层交换机当二层交换机使用。

根据上面的描述，按道理这时在电脑PC的“命令行”中执行命令“telnet 192.168.2.2”后，就能登录到Cisco3750上，因为IP地址192.168.2.2是3750的管理地址。但结果没能登录成功，并且还发现三点奇怪的现象：一是在PC的“命令行”中执行命令“telnet 192.168.2.254”却能登录成功，也就是说从PC上能成功Telnet到Cisco4506上，却Telnet不上Cisco3750上；二是在Cisco4506上也能Telnet到Cisco3750上，也就是在4506上执行命令“Cisco4506#telnet 192.168.2.2”却能成功登录到3750；三是在PC上能ping通4506上接口VLAN 2的IP地址192.168.2.254，但ping不通3750的IP地址192.168.2.2。如下所示是在PC的“命令

```
  1     1 ms    <1 毫秒    <1 毫秒  PCoS-2011030WR [192.168.11.254]
  2      *       *          *         请求超时
  3      *       *          *         请求超时
```

上面的输出在第“3”行的下面本来还有很多，都省略了。因为数据包不能成功到达目的地192.168.2.2，所以它只能像第“3”行那样往下延续地输出。从输出的结果可以看出，PC上发出的数据包只能到达Cisco4506上，因为第“1”行输出中的192.168.11.254就是4506上VLAN 11的IP地址。然后，Telnet数据包从4506上，就不能路由到Cisco3750上，因为从第“2”行输出，一直返回不到数据包。所以可以确定Telnet故障的部位就在Cisco4506和Cisco3750之间，又因为用户的PC可以正常访问网络，所以又可以排除是网络线路的故障。

最终认为可能是Cisco3750上的故障，查看3750的配置文件，发现其中没有默认路由的配置，也就是没有类似“ip default-gateway”和“ip route 0.0.0.0 0.0.0.0”的命令，这两个命令前者是在三层交换机关闭路由功能或者路由功能模块损坏的情况下才有效，而后者是启用了三层交换机的路由功能后，配置默认网关的命令。两个命令的功能都是一致的，路由器在路由表中找不到对应的路由项，就会依照默认网关把数据包发送出去。

既然Cisco3750上没有配置默认网关，所以从PC上发出的Telnet数据包，通过Cisco4506路由，最终到达Cisco3750上后，它不知道怎样把数据包发送出去，因为交换机根本就没有配置这方面的命令。所以它只能把Telnet数据包作丢弃处理。最终电脑PC也就收不到Cisco3750返回的数据包，导致不能ping和Telent成功。

在Cisco3750上执行命令“Cisco3750(config)#ip default-gateway 192.168.2.254”后，PC可以正常登录到3750上，故障消失。

2. Telnet故障实例二

如图8-7所示，是公司的一台Cisco3750发生故障，需要登录到交换机上排除故障的网络图示。网络的连接非常简单，就是用一台PC通过网线连接到Cisco3750上。其中PC的IP地址为192.168.2.9，子网掩码为255.255.255.0，它通过Cisco3750的Gi1/0/24和交换机相连。其实要对Cisco3750进行配置，可以用

```
C:\Users\Administrator>ping 192.168.2.3
正在 Ping 192.168.2.3 具有 32 字节的数据:
来自 192.168.2.3 的回复: 字节=32 时间<1ms TTL=255
来自 192.168.2.3 的回复: 字节=32 时间<1ms TTL=255
来自 192.168.2.3 的回复: 字节=32 时间<1ms TTL=255
来自 192.168.2.3 的回复: 字节=32 时间=1ms TTL=255
192.168.2.3 的 Ping 统计信息:
数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，往返行程的
估计时间(以毫秒为单位):最短 = 0ms，最长 = 1ms，平均 = 0ms
```

从上面的输出可以看出PC和Cisco3750之间的网络是通的，因为可以ping通。所以觉得不能Telnet成功，故障还是出在Cisco3750交换机上，进一步查看配置文件，发现在虚拟端口的配置中有一项“transport input none”，如下所示：

```
line vty 0 4
 password 7 121254631595C517E
transport input none
 login
line vty 5 15
 password 7 121254631595C517E
transport input none
 login
```

查资料发现命令“transport input none”的作用是不允许任何协议和这台交换机建立连接，即用户不能远程登录到这台交换机了。问题应该就出在这里，在虚

8.3　运维实例：UDP/TCP调试助手应用

UDP/TCP调试助手是一个辅助调试UDP/TCP的工具软件，支持TCP Server、TCP Client、UDP通信模式，为网络调试提供了极大的方便。它也是一款绿色软件，只需把程序拷贝到电脑上就能使用，如图8-8所示。

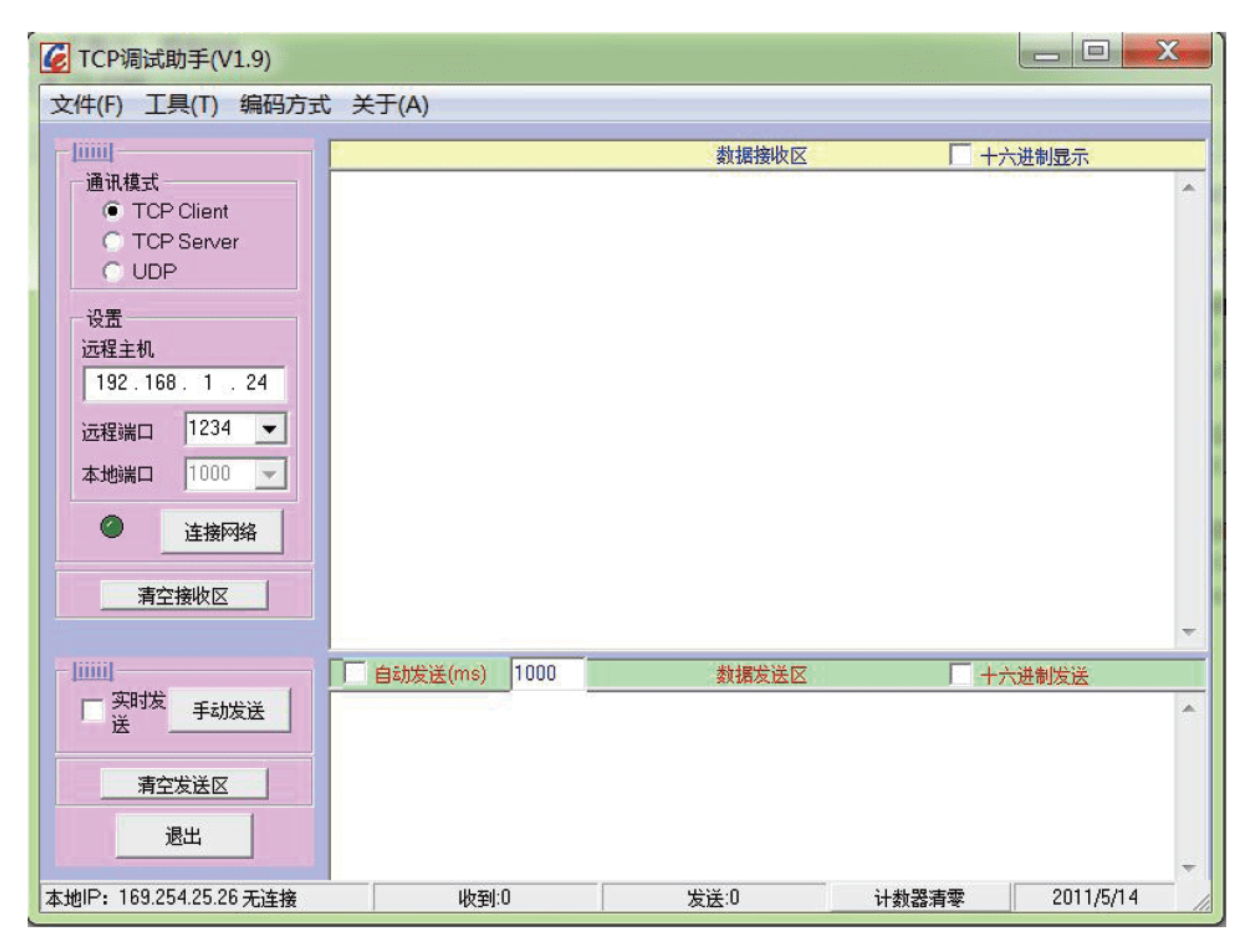


图8-8　TCP调试助手V19

运行平台：Windows XP/2003/Vista/7

软件授权：免费软件/调试工具

软件大小：1550KB

首先，若要测试网络上两个终端的TCP服务是否正常，只需在两个终端上分别选择好调试助手的Client和Server模式。在TCP Client一端，要填上“远程主

机”的IP地址，“远程端口”号。在TCP Server一端，要填上“远程主机”IP地址，“本地端口”号。测试时，首先在Server端的UCP/TCP调试助手上单击“开始监听”，然后在Client端的UCP/TCP调试助手上单击“连接网络”。然后在两个终端上的调试助手的对话框中就可以发送一些文字来测试网络的TCP服务是否正常。其次，若要测试两个网络终端的UDP服务是否正常，只需在两端调试助手的“远程主机”、“远程端口”和“本地端口”输入对应的参数，然后单击“开启UDP”，就可以测试UDP服务了。